

Safety Evaluation With Open Items

U.S. EPR Design Certification

Chapter 7 – Instrumentation and Control Systems

ENCLOSURE

# CONTENTS

<b>Contents .....</b>	<b>ii</b>
<b>List of Figures .....</b>	<b>iii</b>
<b>List of Tables .....</b>	<b>iv</b>
<b>List of Acronyms .....</b>	<b>v</b>
<b>7.0 Instrumentation and Controls .....</b>	<b>1</b>
7.1 Instrumentation and Controls – Introduction .....	1
7.2 Reactor Trip System .....	76
7.3 Engineered Safety Features Systems .....	88
7.4 Systems Required for Safe Shutdown .....	116
7.5 Information Systems Important to Safety .....	124
7.6 Interlock Systems Important to Safety .....	137
7.7 Control Systems Not Required For Safety .....	148
7.8 Diverse I&C Systems .....	174
7.9 Data Communication Systems .....	233

## LIST OF FIGURES

Figure 7.1-1 Service Unit Implementation in U.S. EPR.....	60
Figure 7.7-1 I&C Signal Flow Path From Sensor to Control Rods .....	164
Figure 7.8-1 Legend Applicable to all Figures of this Section .....	178
Figure 7.8-2 TXS System Application Software.....	<b>Error! Bookmark not defined.</b>
Figure 7.8-3 Automatic D3 Mitigation Block Diagram .....	<b>Error! Bookmark not defined.</b>
Figure 7.8-4 D3 I&C Mitigation Credited by the Staff.....	<b>Error! Bookmark not defined.</b>
Figure 7.8-5 ATWS Mitigation Systems.....	<b>Error! Bookmark not defined.</b>
Figure 7.8-6 Example of the PS ESF Actuation Signal Path for One Division.....	226
Figure 7.9-1 Interface between U.S. EPR I&C Safety Systems and PICS ..	<b>Error! Bookmark not defined.</b>
Figure 7.9-2 Depiction of Logical Connections within One Division of PS..	<b>Error! Bookmark not defined.</b>

## LIST OF TABLES

Table 7.1-1 Self-Testing Features in U.S. EPR Design .....	50
Table 7.1-2 Conformance to RG 1.62 Regulatory Positions .....	68
Table 7.2-1 Section 7.2 References to Other Report Sections .....	78
Table 7.2-2 Reactor Trip Functions .....	82
Table 7.2-3 Permissives .....	84
Table 7.3-1 Section 7.3 References to Other Report Sections. ....	92
Table 7.3-2 ESF Actuation Functions .....	96
Table 7.3-3 Permissives and Operating Bypasses .....	100
Table 7.4-1 Section 7.4 References to Other Report Sections .....	118
Table 7.5-1 Section 7.5 References to Other Report Sections .....	129
Table 7.6-1 Section 7.6 References to Other Report Sections. ....	141
Table 7.7-1 Section 7.7 References to Other Report Sections. ....	151
Table 7.7-2 RCSL Control Features .....	160
Table 7.7-3 PAS Major Control Functions .....	168
Table 7.8-1 References to Other Sections of the Report. ....	177
Table 7.8-2 PS-DAS Diversity Attributes Credited by the Staff .....	182
Table 7.8-3 PAS and SAS Automatic System Control Functions .....	185
Table 7.8-4 Summary of PAS-PS Diversity Attributes .....	188
Table 7.8-5 Summary of SAS-PS Diversity Attributes .....	191
Table 7.8-6 Credited D3 Manual Controls Available in the Main Control Room .....	194
Table 7.9-1 Section 7.9 References to Other Report Sections .....	236
Table 7.9-2 Summary of Data Communications Implementation for Safety Systems .....	247
Table 7.9-3 Evaluation of the U.S. EPR Safety System Interdivisional Communication .....	258
Table 7.9-4 Evaluation of Data Communication Between Safety and Non-safety Systems ....	271

## LIST OF ACRONYMS

10 CFR	Title 10 Code of Federal Regulations
12-UPS	12-hour Uninterruptible Power Supply
ACT	average coolant temperature
ADM	anti-dilution mitigation
ALU	Acquisition Logic Unit
AMI	Accident Monitoring Instrumentation
AMS	Aeroball Measurement System
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrence
APU	Acquisition and Processing Unit
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
AUs	acquisition units
BCMS	Boron Concentration Measurement System
BOC	beginning of cycle [PM Confirm]
BTP	Branch Technical Position
CCF	Common Cause Failure
CCWS	Component Cooling Water System
COT	Core Outlet Thermocouple
CRC	Cyclic Redundancy Check
CRDCS	Control Rod Drive Control System
CRDM	Control Rod Drive Mechanism
CU	Control Unit
CVCS	Chemical Volume Control System
DAS	Diverse Actuation System
DAU	diverse actuation unit
DBE	Design Basis Event
DCS	Distributed Control System
DNBR	Departure from Nucleate Boiling Ratio
DPRAM	Dual-Port Random Access Memory
EATs	emergency auxiliary transformers
EBS	Extra Borating System
ECSS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EFW	Emergency Feedwater
EIS	Ex-core Instrumentation System
EIA	Electronic Industries Alliance
EMI	Electromagnetic Interference
EOC	end of cycle [PM Confirm]
EPSS	Class 1E Power Supply System
ESD	Electrostatic Discharge
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Features Actuation System
EUPS	Class 1E Uninterruptible Power Supply
FDG	Function Diagram Group
FMEA	Failure Modes and Effects Analysis
FMS	Fatigue Monitoring System

FPGAs	Field Programmable Gate Arrays
FR	Federal Register
FSAR	Final Safety Analysis Report
GDC	General Design Criteria
GL	Generic Letter
GW	Gateway
HFE	Human Factors Engineering
HLPD	High Linear Power Density
HMI	Human-Machine Interface
HMS	Hydrogen Measurement System
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
ICIS	In-Core Instrumentation System
IEC	International Electrotechnical Commission
I/O	Input/Output
ISA	Instrument Society of America
ISG	Interim Staff Guidance
ITAAC	Inspections, Tests, Analyses and Acceptance Criteria
LBLOCA	large break loss-of-coolant accident
LDNBR	Low Departure from Nucleate Boiling Ratio
LOCA	Loss-of-Coolant Accident
LDS	Leak Detection System
LPD	Linear Power Density
LPMS	Loose Parts Monitoring System
LRF	Large Release Frequency
LTOP	Low Temperature Over-Pressure
MCR	Main Control Room
MDNBR	Minimum Departure from Nucleate Boiling Ratio
MHSI	Medium Head Safety Injection
MOVs	Motor Operated Valves
MSI	Monitoring and Service Interface
MSRT	Main Steam Relief Train
MW	Megawatt
NATs	normal auxiliary transformers
NMS	Neutron Monitoring System
NRC	U.S. Nuclear Regulatory Commission
NQA	nuclear quality assurance [PM Confirm]
NUPS	non-Class 1E uninterruptible power supply
PA	Postulated Accident
PACS	Priority and Actuator Control System
PAM	Post-Accident Monitoring
PAMS	Post-Accident Monitoring System
PAS	Process Automation System
PCT	peak cladding temperature
PDIL	Power Dependent Insertion Limit
PICS	Process Information and Control System
PLD	Programmable Logic Device
PS	Protection System
PSAI	plant-specific action item
QAP	Quality Assurance Plan
QDS	Qualified Display System

RAI	Request for Additional Information
RCCA	Rod Control Cluster Assembly
RCS	Reactor Coolant System
RCSL	Reactor Control, Surveillance, and Limitation
RFI	Radio Frequency Interference
RG	Regulatory Guide
RHR	Residual Heat Removal
RHRS	Residual Heat Removal System
RMS	Radiation Measurement System
RPMS	Rod Position Measurement System
RPV	Reactor Pressure Vessel
RPVDT	Reactor Pressure Vessel Dome Temperature
RPV LMS	Reactor Pressure Vessel Level Measurement System
RSS	Remote Shutdown Station
RT	Reactor Trip
RTB	Reactor Trip Breakers
RTE	Run Time Engine
RTE	Run-Time Environment
RTS	Reactor Trip System
SAS	Safety Automation System
SBLOCA	small break loss-of-coolant accident
SCCF	Software Common-Cause Failure
SCDS	Signal Conditioning and Distribution System
SDOE	Secure Development and Operational Environment
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SICS	Safety Information and Control System
SMS	Seismic Monitoring System
SPND	Self-Powered Neutron Detector
SRP	Standard Review Plan
SSC	Structure, System, and Component
SU	Service Unit
TBS	Turbine Bypass System
TG	turbine generator
TG I&C	Turbine and Generator Instrumentation and Control
TMI	Three Mile Island
TS	Technical Specifications
TXS	TELEPERM XS
UPS	uninterruptible power supply
V&V	Verification and Validation
VMS	Vibration Monitoring System

## 7.0 INSTRUMENTATION AND CONTROLS

This chapter describes the instrumentation and controls (I&C) for the U.S. EPR design. The description of I&C systems includes system classifications, functional requirements and assignment, and system architecture. The information provided emphasizes those instruments and associated equipment that constitute the safety systems as defined in Title 10 Code of Federal Regulations (10 CFR) 50.55a(h), the General Design Criteria (GDC) of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," and other I&C-related regulations in 10 CFR Part 50.

### 7.1 Instrumentation and Controls – Introduction

#### 7.1.1 Introduction

The U.S. EPR I&C systems provide proper control of plant processes to protect against unsafe and improper reactor operations during steady-state and transient power operations. The I&C systems also provide initiating signals to mitigate the consequences of accident conditions.

#### 7.1.2 Summary

**FSAR Tier 1:** FSAR Tier 1 information associated with this section is found in U.S. EPR Final Safety Analysis Report (FSAR) Tier 1, Section 2.4, "Instrumentation and Control Systems."

**FSAR Tier 2:** The applicant provided a system description in FSAR Tier 2, Section 7.1, "Introduction," which is summarized in the following discussion.

I&C safety systems are the systems that are relied on to remain functional during and following design-basis events to assure: (1) The integrity of the reactor coolant pressure boundary; (2) the capability to shut down the reactor and maintain it in a safe shutdown condition; and (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to 10 CFR Part 100, "Reactor Site Criteria," and/or 10 CFR 50.67, "Accident Source Term," guidelines. Protection systems are a subset of I&C safety systems, and I&C safety systems are a subset of I&C systems important to safety.

The I&C architecture implements several design principles such as defense-in-depth, diversity, redundancy, independence, and deterministic behavior to provide for safety. These principles are applied so that the impact of failures is minimized, and the required safety functions are executed when required.

**ITAAC:** The Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) associated with FSAR Tier 2, Section 7.1, are given in FSAR Tier 1, Section 2.4.

**Technical Specifications:** The Technical Specifications associated with FSAR Tier 2, Section 7.1, are given in FSAR Tier 2, Chapter 16, "Technical Specifications." Specifically, Technical Specifications, Section 3.3, "Instrumentation," addresses I&C systems.

#### 7.1.3 Regulatory Basis

The relevant requirements of the U.S. Nuclear Regulatory Commission (NRC) regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800,



“Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition,” (hereafter referred to as NUREG-0800 or the SRP), Section 7.1, “Instrumentation and Controls – Introduction,” and Appendix 7.1-A, “Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety,” Revision 5, and are summarized below. Review interfaces with other SRP sections can also be found in NUREG-0800, Section 7.1.

- 1 GDC 1, “Quality Standards and Records,” as it relates to assuring structures, systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
- 2 GDC 2, “Design Bases for Protection Against Natural Phenomena,” as it relates to assuring SSCs important to safety shall be designed to withstand the effects of natural phenomena without loss of capability to perform their safety functions.
- 3 GDC 4, “Environmental and Dynamic Effects Design Bases,” as it relates to assuring SSCs important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.
- 4 GDC 13, “Instrumentation and Control,” as it relates to assuring instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.
- 5 GDC 20, “Protection System Functions,” as it relates to the protection system to be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.
- 6 GDC 21, “Protection System Reliability and Testability,” as it relates to assuring the protection system is designed for high functional reliability and inservice testability commensurate with the safety functions to be performed as well as redundancy and independence sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy.
- 7 GDC 22, “Protection System Independence,” as it relates to the design of the protection system to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function.
- 8 GDC 23, “Protection System Failure Modes,” as it relates to assuring the protection system is designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced.

- 9 GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.
- 10 GDC 29, "Protection Against Anticipated Operational Occurrences," as it relates to protection and reactivity control systems to be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.
- 11 10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety," as it relates to assuring systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
- 12 10 CFR 50.55a(h), "Protection and Safety Systems," as it relates to compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the January 30, 1995, correction sheet.
- 13 10 CFR 52.47(b)(1), "Contents of applications; technical information," requires that a design certification contain the proposed inspections, tests, analyses, and acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act of 1954, and NRC regulations.

Acceptance criteria adequate to meet the above requirements include the Standard Review Plan (SRP) Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety, Section 3 (Staff Requirements Memoranda), Section 4 (Regulatory Guides (RG)), and Section 5 (Branch Technical Positions (BTP)), that list the SRP acceptance criteria applicable to I&C systems important to safety.

#### **7.1.4 Technical Evaluation**

Objectives of the staff's review are to confirm that the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; that these functions, the implementing systems, and the equipment have been properly classified; and that the commitments have been made to use appropriate quality standards for the I&C systems.

Several of the design considerations are addressed in this section with references, as appropriate, for information contained in Sections 7.2 through 7.9 of this report.

The staff's review of the I&C systems conducted in this section is based on the docketed FSAR, Revision 2. However, since FSAR Revision 2, was submitted, the applicant made several changes to the I&C system design as part of request for additional information (RAI) responses.

Those new design changes were not a result of the specific response to the RAI that transmitted them to the staff but were incorporated in the mark-ups for FSAR Tier 1, Section 2.4 and FSAR Tier 2, Chapter 7, Interim Revision 3 mark-ups. Specifically, the June 22, 2011, response to RAI 442, Question 07.01-26, provides FSAR Tier 2, Section 7.1, Interim Revision 3 mark-ups, and RAI 452, Question 07.03-36 provides the Interim Revision 3 mark-ups for FSAR Tier 1, Section 2.4. **RAI 442, Question 07.01-26 and RAI 452, Question 07.03-36 are being tracked as confirmatory items.** Unless otherwise noted, references to Interim Revision 3 mark-ups refer to these confirmatory RAI responses.

The following technical evaluation discusses the staff review of the conformance of the proposed design to NRC regulations.

#### *7.1.4.1 Proposed Alternatives to IEEE Std 603-1991*

In a May 24, 2011, letter, the applicant requested NRC approval on two proposed alternatives in accordance with 10 CFR 50.55a(a)(3)(i). The applicant proposed using IEEE Std 603-1998 in lieu of IEEE Std 603-1991, and proposed using a conservative setpoint selection method as an alternative to independence and redundancy requirements with regard to SPND-based reactor trip functions. 10 CFR 50.55a(a)(3) states, in part, that proposed alternatives to the requirements of 10 CFR 50.55a(h) may be used when authorized by the Director, Office of New Reactors. The applicant is required to demonstrate that the proposed alternative would provide an acceptable level of quality and safety. The two proposed alternatives are evaluated below.

##### *7.1.4.1.1 Assessment of the Use of IEEE Std 603-1998*

The purpose of 10 CFR 50.55a(h)(3) is to ensure that nuclear power facilities have adequate criteria with respect to the design, reliability, qualification, and testability of the instrumentation and control portions of power plants. IEEE Std 603-1991 establishes minimum functional and design requirements for the power and instrumentation and control portions of safety systems for nuclear power plants. In an April 13, 1999, Federal Register (FR) Notice, the NRC amended its regulations to incorporate IEEE Std 603-1991, effective on May 13, 1999. The section, "Significant Comments on the Proposed Rule," contained a subsection, "(2) Referenced Standards," which stated:

As a matter of law, the other IEEE standards referenced in IEEE Std 603-1991 are not rulemaking requirements, inasmuch as (i) Section 50.55a does not contain language explicitly requiring the use of the other IEEE standards referenced in IEEE Std 603-1991, and (ii) the other IEEE standards referenced in IEEE Std 603-1991 have not been approved for incorporation by reference by the Office of Federal Register.

Therefore, in the staff assessment of the acceptability of using IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," in lieu of IEEE Std 603-1991 (hereinafter, proposed alternative), a comparison of the referenced standards was not performed, since the standards referenced by IEEE Std 603-1991 are not a rulemaking requirement, which means that these other standards are not required by regulation. Furthermore, IEEE Std 603-1991 and IEEE Std 603-1998 reference other guidance that is not incorporated separately into NRC regulations and, thus, this guidance is not a rulemaking requirement. Therefore, the staff evaluation of the proposed alternative does not include a review and evaluation of any of the guidance documents in IEEE Std 603-1998. The majority of differences in referenced guidance documents between the 1991 and 1998 versions of

IEEE Std 603 is the 1998 version references later revisions of the same guidance documents referenced in IEEE Std 603-1991. The staff assessment discussed below only addresses those clauses in which there are differences in the wording. The clauses for which the wording in IEEE Std 603-1998 is the same as the wording in IEEE Std 603-1991, are not discussed in the following staff assessment, as they provide an acceptable level of quality and safety.

The staff evaluation of the proposed alternative is a separate determination of whether the applicant's design meets the requirements of IEEE Std 603-1998. The staff's review and discussion of whether the applicant's design of the U.S. EPR meets the requirements of IEEE Std 603-1998 is delineated in Sections 7.1 through 7.9 of this report.

On November 24, 2009, the applicant submitted ANP-10309, "U.S. EPR Digital Protection System Technical Report," Revision 0, which contained the applicant's argument that the proposed alternative provides an acceptable level of quality and safety. This was superseded by a May 24, 2011 letter. In support of using IEEE Std 603-1998 in lieu of IEEE Std 603-1991, the applicant evaluated each difference between the IEEE Std 603-1991 and IEEE Std 603-1998, and determined that IEEE Std 603-1998 meets or exceeds the requirements of IEEE Std 603-1991. The staff reviewed the information provided and found that the majority of differences reside in the language to add clarification and/or refer to a guidance document. The staff reviewed and evaluated the information provided by the applicant for the proposed alternative and concluded that the proposed alternative provides an acceptable level of quality and safety.

IEEE Std 603-1998 contains requirements in five sections: Sections 4, 5, 6, 7, and 8. The acceptability of the language used for the definitions in "Paragraph 3 Definitions" of the standard, is evaluated in the context of the impact to the requirements. The details of the staff assessment of the proposed alternative to comply with IEEE Std 603-1998 in lieu of IEEE Std 603-1991 is discussed in the Attachment to this Chapter 7 report.

#### *7.1.4.1.2 Proposed Alternative to IEEE Std 603-1991, Clause 5.6.1*

In Attachment 2 of a May 24, 2011, letter, the applicant proposed an alternative request to use conservative setpoint selection to satisfy the single failure criteria in lieu of IEEE Std 603-1991, Clause 5.6.1. IEEE Std 603-1991, Clause 5.6.1, requires redundant portions of a safety system provided for a safety function to be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring the safety function.

In the design, the Low Departure from Nucleate Boiling Ratio (LDNBR) and High Linear Power Density (HLPD) reactor trip functions are based on 72 Self-Powered Neutron Detector (SPND) measurements. Because each detector occupies a unique location within the core, and flux is not uniform throughout the core, the SPNDs do not operate redundantly to each other. Therefore, redundancy and independence between divisions cannot be used to satisfy the single failure criterion for the SPND input measurement channels. Instead, the applicant requested the use of a conservative setpoint selection method to satisfy single failure requirements for the SPND-based reactor trip functions as an alternative to independence between redundant divisions required by IEEE Std 603-1991 Clause 5.6.1. Clause 5.6.1 is identical in both the 1991 and 1998 versions of IEEE Std 603. Therefore, this request is applicable to both versions of the standard.

Section 1.0, Attachment 2, of the alternative request states that the applicant acknowledges the staff's position that independence provides protection against two types of failures including

(1) single failures postulated in the design and addressed through the system failure modes and effects analysis, and (2) unanticipated failure modes that may not be envisioned or postulated in the design. The applicant states that for the HLPD and LDNBR RT functions, alternative design features which provide reasonable assurance of protection against both of these failure types are used in lieu of redundant and independent sensor measurements between protection system (PS) divisions. A conservative setpoint selection method is used to mitigate postulated single SPND input channel failures.

Section 2.0, Attachment 2, of the alternative request describes the benefits of SPND based core surveillance and protection. This section states, "The use of in-core SPNDs, radially (12 radial locations) and axially (6 elevations along a "string" at each radial location) throughout the reactor core, facilitates direct and accurate on-line monitoring of the core power distribution during steady state and transient conditions. The totality of the 72 measurements is used in three distinct ways:

- Individually, each of the 72 SPNDs measure neutron flux at specific points in the core which allows for continuous monitoring of the local hot spot in the core (HLPD protection).
- Each of the 12 strings of six SPND sensors provides information required to perform detailed axial power shape reconstruction for continuous evaluation of the minimum departure from nucleate boiling ratio (MDNBR) for the hot channel in the core (LDNBR protection).
- Collectively, the 72 SPND signals are arranged geometrically in the core to provide 36 pair of symmetric neutron flux measurements. This allows the protection system to confirm symmetric distribution of power when it exists, and to respond appropriately when asymmetries are detected (imbalance protection)."

Section 2.1, Attachment 2 of the alternative request describes the benefits of using in-core detectors relative to ex-core detectors. This section states that IEEE Std 603-1998, Clause 6.4, requires that to the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis. This clause reflects the fact that reliance on assumptions and application of uncertainties can be reduced by using the most direct available measurement. Due to the location around the periphery of the core, ex-core neutron detectors are most sensitive to the fuel assemblies at the periphery of the core, which are typically not the limiting locations relative to protecting fuel safety limits. Uncertainties and assumptions must then be factored into the ex-core detector measurements to relate the indirect measurements to the calculated real conditions in fuel assemblies closer to the center of the core. The use of 72 in-core SPNDs distributed throughout the core achieves a more direct measurement of core flux, which aligns to the requirements of Clause 6.4 of IEEE Std 603-1998.

Section 2.2, Attachment 2 of the alternative request describes the benefits of using 72 SPNDs in each PS division relative to a divisionalized approach. Two options for a divisionalized approach were considered by the applicant, including (1) four divisions of SPND sensors with the addition of more SPND sensors, such that each division is composed of 72 SPNDs, (2) four divisions of SPND sensors using the existing 72 SPNDs, such that each division is composed of 18 SPNDs. The applicant states that the first option is unfeasible due to spatial limitations in the core to accommodate 216 additional SPNDs. For the second option, the applicant determined

that a hypothetical design solution in which each division would perform HLPD and LDNBR calculations based on 18 SPND measurements would not be prudent for the following reasons:

- The hypothetical design essentially nullifies the advantages of direct measurement. Because each division would only use 18 measurements, those 18 measurements would have to be representative of the entire core. This would result in additional uncertainty in the measurements, similar to using ex-core detectors. Not only would this result in reduced operating margin, it would necessarily result in overly conservative reactor trip (RT) setpoints which would increase potential for unnecessary challenges to the plant safety systems in the form of spurious reactor trips.
- The hypothetical design impairs the ability to detect asymmetric core conditions. Since the LDNBR function is performed on a per-SPND string basis, the six SPNDs on a string must be acquired by one division. The hypothetical design would have three SPND strings acquired by each PS division. This is problematic, because detection of asymmetric events relies on comparison of symmetric pairs of SPNDs across the core.
- The hypothetical design is less robust against multiple failures of SPNDs. If two or three SPNDs, each in a different division are out of service or failed, the ability of multiple divisions to respond to an event is impaired. This is due to the increased “importance” of each SPND to its division’s functions, because the division has a smaller number of SPNDs to begin with. This is in contrast to a design where all 72 measurements are acquired by each PS division, allowing all divisions to perform the function with multiple failed SPNDs, because the contribution of a single SPND is less “important” to the overall function when all four divisions acquire all 72 measurements.

Thus, the applicant concludes that the potential divisionalized designs mentioned above,, while meeting independence requirements at the sensor level, is a less robust design that does not take advantage of the safety benefits provided by more direct measurement. In addition, such a design would have a negative effect on overall plant safety and reliability.

Section 3.0, Attachment 2 of the alternative request describes how the LDNBR and HLPD reactor trip functions comply with the single failure criterion. This section states that each division of the PS receives all 72 measurements for evaluating core conditions. To accomplish this, the SPND signals are amplified and multiplied via analog hardware, and 72 electrically isolated signals are provided to the acquisition and processing units (APU) in each PS division. After acquisition by the APUs, each division of the PS independently performs the HLPD and LDNBR calculations and downstream voting logic. Therefore, the LDNBR and HLPD reactor function exhibit traditional redundancy and independence from APU acquisition of the SPND measurements through the reactor trip breakers. Thus, a single failure within the APU will not cause a loss of the safety function, as that is accommodated by the redundancy within the PS. However, a single failure in an upstream SPND input channel does impact all four PS divisions. Conservative setpoint selection is therefore present in each PS division so that a single failure in a SPND input channel does not prevent any PS division from performing the reactor trip function.

Section 3.0, Attachment 2 further clarifies the categories of single failure for an SPND input channel. This section states that failures in SPND input channels can be grouped into two categories: (1) Those that are automatically detected by the protection system (detected failures) and (2) those that are not (undetected failures). Both failure types can be detected during periodic surveillance testing required by the Technical Specifications. The conservative

setpoint selection approach can be summarized as follows: a detected failure results in an automatic transition to a more conservative setpoint in the PS logic; a single undetected failure is assumed to always exist and is factored into determination of the setpoint values that exist in the PS logic.

Section 3.1, Attachment 2 of the alternative request discusses the mechanisms used to detect SPND failures. This includes monitoring the status of the power supplies to amplifiers and signal multiplication devices, using self-monitoring features built into the APU signal acquisition and analog to digital conversion hardware, monitoring the health and availability of APU analog input modules, and detecting out-of-range signals. A detected failure results in an invalid status being assigned to the affected SPND measurement signal in the PS software in each PS division. If a SPND fault is detected via periodic surveillance testing, the affected signal is manually assigned an invalid status in each PS division. Once a SPND signal is assigned an invalid status, the PS logic automatically selects a more conservative reactor trip setpoint, and this transition is alarmed in the main control room.

Section 3.2, Attachment 2 of the alternative request discusses the accommodation of undetected SPND failures. This section states that there is a low probability of a non-self announcing failure in the SPND amplification and signal multiplication equipment. Although this type of failure would be detected through surveillance testing in the Technical Specifications, this type of failure has the possibility to compromise the integrity of a SPND signal that is used to perform a safety function during the period between the surveillance testing intervals. Therefore, in Section 3.2.1, Attachment 2 of the alternative request, the applicant committed to revise Topical Report ANP-10287P, "In-core Trip Setpoint and Transient Methodology For U.S. EPR Topical Report," to add the method for including the undetected SPND failure. Based on the revised in-core trip set point and transient methodology, the applicant also committed to re-analyze the FSAR Tier 2, Chapter 15 events that take credit for the in-core DNBR and linear power density (LPD) trips and will provide a revision to their Chapter 15 submittals. The staff issued an RAI 505, Question 07.01-33 to request the necessary revisions. **RAI 505, Question 07.01-33 is being tracked as an open item.**

Section 3.2.2, Attachment 2 of the alternative request states that for symmetric events, the reactor trip setpoints will be largely unaffected by the inclusion of an undetected loss of the most limiting SPND response. For asymmetric events, the power distribution will have more localized changes due to the event. Thus, the inclusion of an undetected loss of the most limiting SPND response will, in most cases, require the responses from SPNDs more distant from the location of maximum DNBR degradation to reach the reactor trip setpoint. Therefore, an increase of the LDNBR imbalance/rod drop setpoints will be required to account for loss of the most limiting SPND signal while respecting fuel safety limits. This change in reactor trip setpoints will result in a change in the response of the PS to asymmetric events. The events that credit the LDNBR imbalance/ rod drop functionality will be re-analyzed to account for the change in PS response. The applicant states that the conclusion reached in the safety analysis for these asymmetric events will not be changed with respect to non-violation of safety limits.

Section 4.0, Attachment 2 of the alternative request discusses the protection of the PS against unanticipated failure modes. This section states that the only portion of the PS design where redundancy and independence are not present is the SPND input channels. From the point of acquisition of the SPND measurements through the RT breakers, independence is implemented between redundant divisions. Thus, the applicant is only considering measures included in the design which provide reasonable assurance of protection against unanticipated or multiple failures in the SPND input channels. To protect against software and communication failures,

the design of the SPND input channels uses only analog signal conditioning equipment to amplify and then split each SPND measurement so that four hardwired, analog signals are generated and sent separately to each PS division. Using only analog equipment to provide the measurements to the PS divisions increases confidence that potential failure modes are understood and mitigated in the design. Additionally, this section states that implementing principles of diversity and defense-in-depth in the design, such as the use of two subsystems within the PS and the diverse actuation system (DAS), provide additional protection against unanticipated failure modes of the SPND input channel.

The staff evaluated the proposed alternative to IEEE Std 603-1991, Clause 5.6.1, and has the following conclusions for the proposed alternative:

- The use of 72 SPNDs relative to ex-core detectors provides a more direct measurement of the core conditions, thus allowing a reduction in the level of uncertainty and assumptions used in calculating the core conditions. The staff finds the use of in-core detectors to provide more direct measurements of the core flux is consistent with the requirements of IEEE Std 603-1998, Clause 6.4, which require to the extent feasible and practical, that sense and command features inputs shall be derived from signals that are direct measures of the desired variables.
- The use of 72 shared SPND measurements in each PS relative to a divisionalized approach provides an acceptable design that can enhance plant safety by accommodating multiple sensor input failures and provide more direct measurement of core conditions. Specifically, the staff determined that the spatial limitations in the core prevent the inclusion of 216 additional SPNDs to provide 72 separate SPND inputs to each PS division. In addition, the staff determined that a divisionalized design, in which each division would perform HLPD and LDNBR calculations based on 18 SPND measurements, would not provide a reliable accommodation for asymmetrical events in the core, and multiple SPND failures in one division. Therefore, the staff finds the use of 72 shared SPND inputs in each PS division provides an enhanced design in terms of plant safety and reliability relative to a divisionalized approach.
- The use of conservative setpoint selection in the PS logic provides an acceptable method to accommodate multiple detected SPND failures and a single undetected failure of the most limiting SPND.
- The use of only analog signal conditioning equipment to amplify and then split each SPND measurement into four hardwired, analog signals precludes the introduction of software and communications failures in the SPND input channels that may affect all PS divisions.
- The staff finds that alternative request to IEEE Std 603-1991, Clause 5.6.1, is acceptable upon the satisfactory revisions to the applicant's analysis and documentation. Specifically, the applicant committed to (1) the submission of a revision to Topical Report ANP-10287P to add the method for including the undetected SPND failure and (2) re-analysis of the FSAR Tier 2, Chapter 15 events, that take credit for the in-core DNBR and LPD trips. RAI 505, Question 07.01-33 was issued to request the revisions.  
**RAI 505, Question 07.01-33 is being tracked as an open item.**



#### 7.1.4.2 *Overview of Instrumentation and Controls Systems*

This sub-section outlines the I&C system, also known as the distributed control system (DCS), as submitted by the applicant in the design certification application. The description of the DCS is found in FSAR Tier 2, Chapter 7, Interim Revision 3 mark-ups.

##### 7.1.4.2.1 *System-Level Instrumentation and Controls Architecture*

FSAR Tier 2, Revision 3, Figure 7.1-2, "Distributed Control System Functional Architecture," illustrates the main instrumentation and control systems of the U.S. EPR design used for control and monitoring in the plant, which are collectively referred to as the DCS. The DCS performs the majority of signal input processing, automation, operator interface, annunciation of abnormal process conditions, and actuator output functions in the plant. The DCS also implements functional requirements specified by various plant mechanical and electrical systems.

In the U.S. EPR design, all I&C functions and equipment are categorized as safety-related and non-safety-related according to their functions in the safety analysis. In FSAR Tier 2, Figure 7.1-2, the shaded systems and components are safety-related, and the non-safety-related systems and devices are not shaded.

##### 7.1.4.2.1.1 *Safety-Related Systems*

The following I&C systems of the U.S. EPR design and their associated field sensors, actuators, and other components are safety-related:

- Protection system
- Safety automation system (SAS)
- Safety information and control system (SICS)
- Priority and actuator control system (PACS)
- Signal conditioning and distribution system (SCDS)
- Auxiliary components and black box systems

#### Protection System

As shown in FSAR Tier 2, Figure 7.1-2, the PS is an integrated system which consists of the reactor protection system and engineered safety features (ESF) actuation system. The PS detects plant conditions that indicate the occurrence of anticipated operational occurrences (AOOs) and postulated accidents (PAs), and it actuates the safety-related process systems required to mitigate the events. Implemented with the TELEPERM XS (TXS) platform, the PS is the main I&C line of defense. The primary function of the PS is to bring the plant to a controlled state if a design basis event (DBE) occurs. Tripping the reactor, actuating containment isolation, and initiating emergency core cooling system (ECCS) are some of the main functions provided by the PS. The PS reactor trip function uses voting logic to screen out potential upstream failures of sensors or processing units.

The PS is located in dedicated cabinets in the nuclear island. The PS is organized into four redundant, independent divisions located in separate Safeguard Buildings. Each division

contains two functionally independent subsystems (A and B), with each division powered by its respective Class 1E power source. Additionally, each PS cabinet is provided with its redundant power supplies for the electronic devices and modules. The PS is designed to be functionally independent of all other I&C systems. Connections with other I&C systems are implemented through isolation devices. The PS can perform its own internal self-diagnostics functions and alert the operators to unusual conditions or internal failures.

### Safety Automation System

SAS is a safety-related system dedicated to performing safety-related automatic and manual grouped control functions during normal operations, mitigating the effects of AOOs and PAs, and achieving and maintaining safe shutdown. SAS is implemented with the TXS platform as well. It receives process data from plant instrumentation and switchgear via SCDS, sends actuation signals to PACS for signal prioritization and drive actuation, and transfers monitoring signals to SICS and process information and control system (PICS). SAS also sends hardwired signals to the process automation system (PAS) to coordinate logic for related actuators within the PAS. SAS is organized into four independent divisions, which are located in separate Safeguard Buildings, Emergency Power Generating Buildings, and Essential Service Water Pump Buildings. Each SAS division is powered by its respective Class 1E uninterruptible power supply.

### Safety Information and Control System

SICS is a safety-related human-machine interface (HMI) system which consists of both safety-related and non-safety-related equipment. SICS provides control capabilities in the main control room (MCR) and limited control capabilities in the remote shutdown station (RSS). SICS is specifically designed to provide the operator the necessary controls and indications in the MCR to mitigate the effects of AOOs and PAs concurrent with or without a software common cause failure (SCCF) of the PS, and severe accidents. SICS is also used by the operator in both the MCR and RSS to reach and maintain safe shutdown.

SICS in the MCR is not normally used by the operator, but is used when the PICS is not available. SICS is also used during normal operation for some controls which are not available on the PICS (such as manual RT, ESF actuation, and permissive acknowledgement). SICS in the RSS is used to operate controls which are not available on the PICS in the RSS to reach and maintain safe shutdown following an evacuation of the MCR.

Both safety-related and non-safety-related controls on the SICS are implemented with hardwired buttons and switches. Indications for both safety-related and non-safety-related functions on the SICS are provided via dedicated indicators. A limited number of indications are provided on the non-safety-related qualified display system (QDS) workstations. The QDS workstation consists of a display, computer, and input devices and is capable of trending information, including Type A, B, and C post-accident monitoring (PAM) variables, to provide situational awareness for the operator.

### Priority Actuation and Control System

PACS is a safety-related system that includes both safety-related and non-safety-related equipment. PACS performs prioritization of actuation signals from different safety and non-safety-related DCS systems, drive actuation, and monitoring of plant actuators. The PACS is divided into four independent divisions located in the Safeguard Buildings, Emergency Power Generating Buildings, and Essential Service Water Pump Buildings. There is safety-related and

non-safety-related PACS equipment to interface with safety-related and non-safety-related actuators/black-box systems, respectively.

PACS receives actuation orders from various DCS systems for prioritization. Signals for the PACS are sent via a dedicated data connection from the PAS and hardwired connections from other associated DCS systems. Interfaces with actuation devices and actuated equipment (e.g., switchgear, torque and limit switches) are via hardwired connections. Priority among actuation requests from various DCS systems is established by wiring the inputs using the established priority principles.

Each PACS has two major separate components. The first component is the communication module. The second one is the priority module. One priority module and one communication module are provided for each actuator/black-box system. For safety-related PACS equipment, its safety-related priority module interfaces with the safety-related DCS systems (PS, SICS, and SAS) via hardwired connections and with the non-safety-related DAS via hardwired connection with a qualified isolation device. Its non-safety-related communication module interfaces with the non-safety-related PAS through the datalink. For non-safety-related PACS equipment, the priority module interfaces with both the safety-related SICS system and non-safety-related DAS via hardwired connection. Its communication module interfaces with the non-safety-related PAS through the fiber-optic datalink as well.

The communication module hardware, which performs non-safety-related functions, is qualified to the same level as safety-related modules (i.e. the associated circuit). The safety-related priority module implements the logic functions by using programmable logic devices to perform priority control and command termination. The interface within PACS, between the priority module and communication module, is implemented by hardwired, discrete connections.

The safety-related and non-safety-related PACS equipment monitors and controls safety-related and non-safety-related field actuators, respectively. Each actuator is controlled by its dedicated PACS module, which is diverse from the TXS function processors used for the PS. To address SCCFs, the priority logic control module will undergo 100 percent combinatorial proof-of-design testing.

The safety-related PACS and non-safety-related PACS equipment is located in separate cabinets. The safety-related PACS equipment is powered by its division's Class 1E uninterruptible power supply (EUPS), while the non-safety-related PACS equipment in the Safeguard Buildings is powered from the 12-hour uninterruptable power supply (12-UPS). PACS equipment in the Emergency Power Generating Buildings and the Essential Service Water Pump Buildings are powered from an uninterruptible power supply and a diesel-backed source.

## Signal Conditioning and Distribution System

SCDS is a safety-related system which includes safety-related and non-safety-related equipment. The primary functions of the SCDS are signal conditioning and distribution of signals from sensors or black-box systems. SCDS receives hardwired signal inputs from sensors or black-box systems and then sends hardwired signal outputs to the SICS, DAS, PS, SAS, reactor control, surveillance, and limitation (RCSL); and PAS, as needed. Outputs from safety-related SCDS equipment to non-safety-related DCS systems are electrically isolated by the signal distribution modules.

SCDS is designed with four independent divisions which are located in the Safeguard Buildings, Emergency Power Generating Buildings, and Essential Service Water Pump Buildings. In each division, there are safety-related and non-safety-related SCDS equipment to interface with safety-related and non-safety-related sensors or black-box systems, respectively. The safety-related SCDS and non-safety-related SCDS equipment are located in separate cabinets. The SCDS is composed of non-computerized signal conditioning modules and signal distribution modules. Multiple signal conditioning modules or signal distribution modules may be used for a particular signal, depending on the required conditioning and the number of DCS systems to which the output signal is required to be sent.

The safety-related SCDS equipment is powered from its divisional EUPS. The non-safety-related SCDS equipment is located in the Safeguard Buildings and powered from the 12-UPS, while the non-safety-related SCDS equipment located in the Emergency Power Generating Buildings and the Essential Service Water Pump Buildings is powered from an uninterruptible power supply and diesel-backed source.

## Auxiliary Safety-Related Components and Black-Box Systems

The safety-related auxiliary components and black-box systems include various field devices, such as sensors, actuators, switchgears, electrical breakers, and stand-alone I&C systems, which provide inputs to SCDS, and also provide inputs to and receive actuation outputs from the PACS. The black-box systems include the following stand-alone safety-related I&C systems:

- In-core Instrumentation System (ICIS): ICIS measures certain in-vessel parameters. The ICIS consists of safety-related and non-safety-related equipment. The safety-related portion of the ICIS includes SPND and fixed core outlet thermocouple (COT) measurement, while the non-safety-related portion consists of an Aeroball measurement system (AMS) and reactor pressure vessel dome temperature (RPVDT) measurement system.
- Ex-core Instrumentation System (EIS): The EIS monitors neutron flux during power and shutdown modes of operation and provides the neutron flux level signals to the SCDS for signal conditioning and distribution. Three ranges (power range, intermediate range, and source range) of detection are used in EIS.
- Boron Concentration Measurement System (BCMS): BCMS measures the boron concentration in the chemical and volume control system. The measured boron concentration is conditioned and compensated for temperature effects. The resulting signal is sent to SCDS for distribution to various systems within DCS. The signal is used by PS to mitigate the risk of homogeneous and heterogeneous dilution of the reactor coolant system.

- Radiation Monitoring System (RMS): RMS consists of various detectors and processing equipment throughout the plant to monitor process radioactivity, post-accident radioactivity, effluent radioactivity, airborne radioactivity, and area radioactivity. The RMS includes both safety-related and non-safety-related functions which provide the safety-related and non-safety-related signals to SCDS for distribution.
- Hydrogen Monitoring System (HMS): HMS provides monitoring and indication of hydrogen concentrations in the containment atmosphere during design basis accidents, and also monitors both hydrogen concentrations and steam content in the containment atmosphere during beyond design basis accidents.
- Rod Position Measurement System (RPMS): RPMS is a safety-related stand-alone I&C system which measures the position of a rod cluster control assembly located in the reactor vessel. RPMS provides three hardwired position signals to the DCS, which include the lower end rod position and temperature-compensated analog rod position signals to SCDS.

#### 7.1.4.2.1.2 Non-Safety-Related Systems

The following I&C systems of the U.S. EPR design are non-safety-related:

- Process automation system
- Reactor control, surveillance, and limitation system
- Process information and control system
- Diverse actuation system
- Auxiliary components and black-box systems.

#### Process Automation System

PAS is the main automation and control system for the plant. PAS provides control functions for both safety-related and non-safety-related equipment. PAS is segregated into subsystems to account for differences in geographic location within the plant, and design and quality requirements. PAS provides I&C functions for nuclear island subsystems, turbine island subsystems, and balance of plant subsystems. PAS is comprised of four nuclear island divisions for subsystems located in the nuclear island and two trains each for the turbine and balance-of-plant subsystems. These trains are located in the turbine island and balance of plant areas respectively. The PAS is implemented with a computerized industrial digital I&C platform that is diverse from the TXS platform.

#### Reactor Control, Surveillance, and Limitation System

RCSL system provides the functions of automatic reactor limitation functions, automatic and manual reactor operational (control) functions, and core monitoring. When the monitored process parameters deviate from the desired operational values, and before the parameters reach trip set points, the RCSL system would take effect. This action by the RCSL system tends to reduce reactor trips and PS challenges. The RCSL system is organized into four divisions located in separate Safeguard Buildings and is implemented with the TXS platform. The RCSL system is powered from the plant 12-UPS.

## Process Information and Control System

The PICS is an HMI system which is primarily used by the operator during normal, abnormal, and accident operation. However, there are a limited number of controls for PS, SAS, and DAS that are only available on the SICS. The PICS is used to provide the monitoring and control functions of both safety-related and non-safety-related process systems. The safety-related control on the PICS is implemented via the PAS and PACS.

As illustrated in FSAR Tier 2, Revision 3, Figure 7.1-2, "Distributed Control System Functional Architecture," the PICS consists of HMI workstations in both the MCR and the RSS. The PICS workstations with view-only capabilities are provided in the technical service center (TSC) for support of emergency response operations. The PICS also encompasses plant overview panels in both the MCR and TSC. The plant annunciator is integrated into the PICS operating and monitoring system. The PICS displays alarms in the event of abnormalities in processes or systems and provides guidance to the operators in performing the appropriate corrective actions. The PICS is implemented using an industrial I&C platform. The PICS equipment is capable of trending information to provide situational awareness for the operator. In addition, the PICS contains recording capability so that historical data can be recalled by the operator.

## Diverse Actuation System

As shown in FSAR Tier 2, Revision 3, Figure 7.1-2, "Distributed Control System Functional Architecture," the DAS is a non-safety-related system that is provided to mitigate an AOO or PA concurrent with an SCCF of the PS. The DAS is organized into four redundant divisions located in separate Safeguard Buildings. Each division of the DAS contains a diverse actuation unit. Hardwired signals are acquired from the SCDS. The DAS will be implemented with either an electrical, an electronic, or a programmable electronic I&C technology which is not microprocessor based. The non-microprocessor based DAS I&C technology is diverse from the microprocessor-based TXS platform used for the safety-related PS and SAS systems. The DAS is powered from the plant 12-UPS and the station blackout diesel generators in the event of a loss of offsite power.

## Auxiliary Components and Black-Box Systems

The non-safety-related auxiliary components and black-box systems interface with non-safety-related DCS systems. Besides various non-safety-related field devices, such as sensors, actuators, switchgears, and electrical breakers, the black-box systems include the following stand-alone non-safety-related systems:

- Control Rod Drive Control System (CRDCS): The CRDCS is classified as a non-safety-related system; however, its trip contacts are safety-related. The CRDCS is used to control the actuation of the 89 rod cluster control assemblies (RCCAS) in the reactor vessel.
- Reactor Pressure Vessel Level Measurement System (RPVLMS): The RPVLMS provides an indication to the operator of the water level in the reactor vessel for use in the PAM system. The RPVLMS instrumentation primarily includes four probes containing three thermocouple sensors each for the level measurement.
- Seismic Monitoring System (SMS): The SMS produces a permanent record of the vibratory ground motion from various areas of the plant during an earthquake. The SMS is provided to promptly evaluate the seismic response of the plant features important to

safety after an earthquake. The shutdown of the plant is required if vibratory ground motion exceeding that of the operating basis earthquake occurs or if significant plant damage occurs.

- Loose Parts Monitoring System (LPMS): The LPMS detects, locates, and analyzes detached or loosened parts and foreign bodies in the reactor coolant system (RCS) and the secondary side of the steam generators during normal plant operation.
- Vibration Monitoring System (VMS): The VMS monitors changes in the vibration behavior of the reactor pressure vessel (RPV) and its internals, the primary system components, the main coolant pumps, and portions of the main steam line structures in the secondary system by monitoring the frequencies and amplitudes of service-induced component and fluid vibrations.
- Fatigue Monitoring System (FMS): The FMS is provided to record actual fatigue loading conditions on plant equipment. It measures various plant parameters such as temperature and pressure to calculate actual stress loads on major plant components.
- Leak Detection System (LDS): The LDS, in conjunction with other associated systems, promptly detects, quantifies, and localizes leakage from the reactor coolant pressure boundary and selected portions of the main steam system.
- Turbine and Generator (TG) Instrumentation and Control : The TG I&C system regulates the operation of the turbine generator for power generation. The TG I&C also performs a turbine trip when requested by either the PS or DAS. The TG I&C system includes the TG control, speed control, load control, valve control, overspeed protection, turbine supervisory instrumentation, and control of other auxiliary protective subsystems. The TG control is a fault-tolerant control system, which provides many control functions for the TG system, such as automatic TG startup and shutdown control functions, trip logic, and automatic synchronization. The speed control is used during startup and has a minimum adjustable setpoint range of zero to 100 percent of rated speed. The load control is used during normal operation and has a setpoint range of zero to 100 percent of maximum capability. The load control function controls megawatts (MW) based on the plant MW setpoint signal provided by the PAS. The valve control is provided to regulate the flow of main steam entering the HP turbine via four stop valves and four governing control valves. Each stop valve is controlled by an electro-hydraulic actuator. The overspeed control is included to quickly close the main stop, control, reheat stop, and intercept valves in the event of an unsafe condition or to provide overspeed protection. The turbine supervisory instrumentation is provided to monitor thermal, hydraulic and electrical parameters, control equipment components, and initiate automatic alarms and shutdown of the TG system in the event of an unsafe condition. The TG I&C system is implemented in a proprietary digital platform supplied by the TG vendor.

#### *7.1.4.2.2 Data Communication Systems*

The data communication systems are an integral part of both the DCS safety and non-safety-related systems. Each DCS system using data communication in the U.S. EPR design certification application manages its own internal exchanges (including data exchange between divisions) without using external resources. As shown in FSAR Tier 2, Revision 3, Figure 7.1-2, "Distributed Control System Functional Architecture," communication between the

different DCS systems is performed via hardwired connection, point-to-point data connection or networked data connection. Communication within a DCS system is an integral part of that system. For the U.S. EPR design, the data communication system addresses the data communication functions from the following three aspects:

- Data communication among safety-related DCS systems
- Data communication between safety-related and non-safety-related DCS systems
- Data communication among non-safety-related DCS systems

#### 7.1.4.2.2.1 Data Communication Among Safety-Related DCS Systems

Data communication within each safety-related DCS system (PS and SAS) for the U.S. EPR design is based on the TXS communication process as described in Topical Report EMF-2110(NP)(A), "TELEPERM XS: A Digital Reactor Protection System," Revision 1. Topical Report EMF-2110 was found acceptable by the staff for referencing in license applications by an independent safety evaluation on May 5, 2000. Data communication between different safety-related DCS functions is implemented either through point-to-point bi-directional and uni-directional datalinks or through bi-directional ring networks. Intradivisional or interdivisional data communications are also used between safety-related I&C functions for each safety-related DCS system. Within the safety-related SICS system, all the controls and indications are hardwired. The non-safety-related QDS units of the SICS for all four divisions receive data from the PS via a uni-directional point-to-point data connection. There is no data communication in the safety-related SCDS which uses hardwired connection. For the safety-related PACS, there is no data communication between the PACS and other safety-related DCS systems; only hard-wired connections.

#### 7.1.4.2.2.2 Data Communication Between Safety and Non-Safety Related DCS Systems

In the U.S. EPR design certification application, the data communication from the safety-related DCS systems to non-safety-related DCS systems is achieved by using uni-directional data connection implemented between the monitoring and service interface (MSI) unit and a gateway (GW). This includes data communication from safety-related SAS and PS to various non-safety-related DCS systems via the non-safety-related PICS automation bus. Temporary bi-directional data communication can be established on an as-needed basis between safety-related SAS/PS and the service unit (SU) through the MSI for monitoring, diagnostic, parameters changes, and software modification purposes. When the connection is needed, the SU can only be connected to one division of PS or SAS each time. The communication path between the SU and the divisional MSIs for PS and SAS is isolated by hardwired disconnects using a key-operated isolation switch. The GW performs communication protocol translation between the TXS protocols used for safety-related DCS systems and the protocol used for the PICS automation bus. For the safety-related PACS, non-safety-related, bi-directional, and networked data connections are implemented using the non-safety-related communication modules and fiber-optic cables within the PACS and the PAS.

#### 7.1.4.2.2.3 Data Communication Among Non-Safety-Related DCS Systems

As indicated in FSAR Tier 2, Revision 3, Figure 7.1-2, "Distributed Control System Functional Architecture," data communication among the non-safety-related DCS systems is implemented through the plant automation bus as well as through direct hardwired connections or point-to-point data connections via GWs. The plant automation bus also interfaces with the HMI bus



within the PICS system via a pair of servers. This HMI bus also provides uni-directional interface with the plant external information and business systems via firewalls

#### 7.1.4.3 *Quality Standards and Records*

10 CFR 50.55a(a)(1), and 10 CFR Part 50, Appendix A, GDC 1, require structures, systems, and components to be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. In order for the staff to evaluate whether the U.S. EPR design met the requirements of 10 CFR 50.55a(a)(1), and 10 CFR Part 50, Appendix A, GDC 1, the staff used guidance as found in SRP Section 7.1, SRP Appendix 7.1-A, and SRP Table 7-1, "Regulatory Requirement, Acceptance Criteria, and Guidelines For Instrumentation and Control Systems Important to Safety." In regard to 10 CFR 50.55a(a)(1), the guidance in SRP Appendix 7.1-A indicates that the staff is to determine whether the applicant commits to follow the RGs and standards referenced in the SRP Sections 7.1 and that the design should conform to all RGs and standards committed to by the applicant. In regard to GDC 1, the guidance in SRP Appendix 7.1-A indicates that the staff is to confirm that the appropriate RGs and endorsed standards are identified as applicable for each I&C system important to safety. In regard to 10 CFR 50.55a(a)(1) and GDC1, the guidance in SRP Section 7.1 indicates that the review should confirm that the applicant includes (1) a discussion regarding the applicability of each of the criteria and guidelines for each system important to safety, and (2) a statement that the criteria and guidelines are implemented or will be implemented in the design of the I&C systems important to safety.

The applicant commits to conform to the RGs and standards referenced in the SRP Sections 7.1 through 7.9. The staff notes that FSAR Tier 2, Section 1.9.1, "Conformance with Regulatory Guides," states that FSAR Tier 2, Table 1.9-2, "U.S. EPR Conformance with Regulatory Guides," provides a conformance assessment of the RGs as they apply to the U.S. EPR design certification. The staff's review of FSAR Tier 2, Table 1.9-2 confirmed the applicant committed to conform to the RGs referenced in the SRP Sections 7.1-7.9. Additionally, the staff found that FSAR Tier 2, Section 7.1.2.4, "Conformance to Regulatory Guides," and FSAR Tier 2, Table 7.1-2, "I&C System Requirements Matrix," indicate the applicable I&C systems and corresponding RGs and standards for which the applicant commits conformance.

The applicant commits to conform to the BTPs in SRP Table 7-1. The staff notes that FSAR Tier 2, Section 1.9.2, "Conformance to the Standard Review Plan," states that the commitment to conform to the BTPs is found in Technical Report ANP-10292, "U.S. EPR Conformance with Standard Review Plan (NUREG-0800) Technical Report," Revision 1. The staff reviewed Technical Report ANP-10292, "U.S. EPR Conformance with Standard Review Plan (NUREG-0800)," Table 1-2, and concluded that the applicant commits to conform to the BTPs in SRP Table 7-1.

Based on the initial review of the system design for conformance to NRC guidelines, the staff concluded that additional information was required to demonstrate that there is reasonable assurance that the I&C systems fully conform to the guidelines. In RAI 285, Question 07.01-16, the staff requested that the applicant identify the ITAAC that verifies the TXS platform is installed in accordance with the approved TXS topical report, and as necessary, provide corresponding updates to the U.S. EPR FSAR. The staff also requested that the applicant provide details regarding any modifications to the TXS platform design, processes, hardware, and software, since the TXS topical report was approved by the staff in May 2000. In a

February 19, 2010, response to RAI 285, Question 07.01 16, the applicant stated that FSAR design certification application does not contain this detailed information, and that the application is intended to support current and future versions of the TXS platform. The response also mentioned the use of ITAAC on a plant specific basis. The staff finds that any changes to the TXS platform would be performed under the applicant's 10 CFR Part 50, Appendix B quality assurance program. Through vendor and other applicable inspections, the staff could verify the appropriateness of these design changes. Any changes to the TXS platform that affect the design description as found in FSAR would be addressed through the appropriate regulatory change process. Therefore, the staff finds the applicant's February 19, 2011, response to RAI 285, Question 07.01-16 sufficient and considers it resolved.

FSAR Tier 2, Section 7.1.2.2.1, "GDC 1 – Quality Standards and Records," states that the applicable I&C systems listed in FSAR Tier 2, Table 7.1-2 shall be designed to meet the requirements of GDC 1 by complying with IEEE Std 603-1998, Clause 5.3, "Quality." FSAR Tier 2, Table 7.1-2, lists the following systems as safety systems and comply with 10 CFR 50.55a(a)(1) and GDC 1: SICS, PS, SAS, PACS, ICIS, EIS, BCMS, RPMS, HMS, RMS and SCDS. FSAR Tier 2, Table 7.1-2, also lists the CRDCS and RPYLMS as complying with 10 CFR 50.55a(a)(1) and GDC 1.

In RAI 286, Question 07.08-9, the staff requested that the applicant justify why the PICS does not need to meet 10 CFR Part 50, Appendix A, GDC 1. The question indicated that the staff identified throughout Chapter 7 of the U.S. EPR application that PICS is the system that the operators will normally use to monitor and control plant safety systems during all conditions of plant operational states, including normal operation, AOO, postulated accidents, and beyond DBEs. Additionally, the staff noted that PICS provides functions that address the requirements of GDC 13 (e.g., alarms) and GDC 19 (e.g., PAM), as well as diverse actuation functions provided there is an SCCF of the PS. The applicant classifies the PICS as non-safety, supplemented grade (NS-AQ), in FSAR Tier 2, Chapter 3, "Design of Structures, Components, Equipment and Systems," Table 3.2.2-1, and that items with supplemented grade quality are those deemed important to safety by the staff. In RAI 286, Question 07.08-9, the staff also requested that the applicant provide information as to the quality standards to which PICS will be designed and tested. As one example, if PICS is credited for diverse actuation, the applicant should address the applicability of Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related," and its enclosure as one potential standard/guidance. Additionally, the staff requested that the applicant describe compliance to GDC 1 for systems that support PICS and enable its proper operation. The applicant subsequently inserted criteria for PICS augmented quality into FSAR Tier 2, Section 7.1.1.3.2, "Process Information and Control System." The augmented quality criteria for PICS includes the augmented quality assurance program as described in Topical Report ANP-10166A, "AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR Topical Report," Addendum A, "Non-Safety Related Products and Services," and a commitment to prescribed software development processes and activities. While the applicant did not make a statement in its FSAR that PICS is in compliance to GDC 1, the applicant did provide discussion on the PICS augmented quality criteria. The staff considers the PICS augmented quality criteria to be Tier 2\* information. Designating the PICS augmented quality criteria as Tier 2\* information provides reasonable assurance that the PICS will be design, installed, and maintained at an acceptable quality level. Based on the commitments for augmented quality, the staff finds that PICS adequately addresses GDC 1.

Based on the applicant's commitments in FSAR Tier 2, the staff finds that U.S. EPR design adequately addresses 10 CFR 50.55a(a)(1) and GDC 1.

#### 7.1.4.4 *Design Bases*

10 CFR 50.55a(h) incorporates by reference IEEE Std 603-1991. As described in Section 7.1.4.1 of this report, the applicant requested to use the 1998 version of the IEEE standard versus the 1991 version. IEEE Std 603-1998, Section 4 addresses the design bases aspects of the U.S. EPR safety I&C systems. The staff's review of Section 4 of IEEE Std 603-1998 is discussed in Section 7.2, "Reactor Trip System," and Section 7.3, "Engineered Safety Features Systems," of this report.

#### 7.1.4.5 *Single Failure Protection*

10 CFR Part 50, Appendix A, GDC 21, requires that the protection system be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. In addition, IEEE Std 603-1998, Clause 5.1 states that the safety system must perform all safety functions required for a design basis event in the presence of (a) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures, (b) all failures caused by the single failure, and (c) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function. In other words, IEEE Std 603-1998, Section 5.1 requires that any single failure within the safety system shall not prevent proper protective action at the system level when required.

The staff reviewed FSAR Tier 2, Section 7.1 and Technical Report ANP-10309, "U.S. EPR Protection System Technical Report," Revision 3, to verify that the single-failure criterion has been appropriately addressed in the I&C systems designs. Specifically, the staff reviewed the following I&C systems to ensure single failure protection: SICS, PS, SAS, PACS, ICIS, EIS, BCMS, RMS, HMS, SCDS, and RPMS. The staff's technical evaluations of the applicable I&C systems are in the subsequent sections.

The staff's evaluation of GDC 21 and IEEE Std 603-1998, Clause 5.1 with respect to the data communication system is discussed in Section 7.9.4.4 of this report.

##### 7.1.4.5.1 *SICS Single Failure Protection*

FSAR Tier 1, Section 2.4.2, "Safety Information and Control System," states that the SICS is a safety-related HMI and is specifically designed to provide the operator with necessary inventory of controls and indications to mitigate AOOs and PAs, and AOOs and PAs concurrent with a SCCF of the PS, and to reach and maintain safe shutdown. Also, the applicant states that SICS is designed so that safety-related functions required for AOOs or PAs are performed in the presence of the single detectable failures within SICS concurrent with identifiable but non-detectable failures, failures caused by the single failure, and failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

FSAR Tier 2, Table 7.1-2, Sheet 5 of 9, lists the SICS as one of the safety-related I&C systems that is designed to conform to RG 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems." In the MCR and RSS, there exists SICS QDS units and SICS

conventional hardwired I&C panels for each of the four independent SICS divisions. FSAR Tier 2, Table 7.1-1, "Levels of Redundancy in I&C Architecture," states that SICS has a redundancy level of four.

Based on the level of redundancy and independence, the staff finds that the SICS design adequately addresses the single failure guidance in RG 1.53, and that FSAR Tier 1, Section 2.4.2, ITAAC Item 4.10, provides a means to verify this design requirement. Therefore, the SICS design meets the requirements of GDC 21 and Clause 5.1 of IEEE Std 603-1998.

#### *7.1.4.5.2 PS Single Failure Protection*

FSAR Tier 1, Section 2.4.1, "Protection System," states that the PS is provided to sense conditions requiring protective action and automatically initiate the safety systems required to mitigate the event. Also, the applicant states that the PS is designed so that safety-related functions required for AOOs or PAs are performed in the presence of the single detectable failures within PS concurrent with identifiable but non-detectable failures, failures caused by the single failure, and failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

FSAR Tier 2, Table 7.1-2, Sheet 3 of 9, lists the PS as one of the safety I&C systems that are designed to meet GDC 21. In addition, FSAR Tier 2, Table 7.1-2, Sheet 5 of 9, lists the PS as one of the safety-related I&C systems that is designed to conform to RG 1.53. FSAR Tier 2, Section 7.1.1.4.1, "Protection System," states that the PS is organized into four redundant, independent divisions located in separate Safeguard Buildings. FSAR Tier 2, Table 7.1-1, states that PS has a redundancy level of four.

A failure modes and effects analysis (FMEA) can be used to demonstrate compliance to the single-failure criterion. IEEE Std 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," Clause 4.1 states that FMEA is a systematic procedure for identifying the modes of failure and for evaluating their consequences. The essential function of a FMEA is to consider each major part of the system, how it may fail (the mode of failure), and what the effect of the failure on the system would be (the failure effect). IEEE Std 352-1987, Section A2.2 states that a FMEA is conducted to determine the effects of each component failure mode on the overall system performance. In this process, the component failure modes that could contribute to unsafe system failure are identified, and necessary action can be taken at this point in the procedure.

Technical Report ANP-10309P, Appendix A provides the PS FMEA. The applicant's FMEA demonstrates that:

- All credible PS failures are detectable (through self-diagnosis or manual surveillance tests).
- No credible single failure will prevent PS actuation.
- No credible single failure will result in spurious PS actuation.
- The PS will fail to the safe state for all credible failures. The safe state for the reactor trip functions is to fail to trip state. The safe state for the ESF functions is to fail as-is.

Technical Report ANP-10309P, Section 7.2 describes the RT voting logic and states that single failures upstream of the acquisition logic unit (ALU) layer could result in an invalid signal being

used in the RT actuation. To accommodate these failures, the PS modifies the voting logic towards actuation. For zero faulty input signals, the RT voting is two out of four. For one faulty input signal, the RT voting is two out of three. For two faulty input signals, the RT voting is one out of two. For three or four faulty input signals, actuation occurs. Technical Report ANP-10309P, Section 7.3 states that the digital signals within the PS carry a value and a status and that when a signal with a faulty status reaches the voting function block, that signal is disregarded through the automatic modification of the vote. Technical Report ANP-10309P, Section 7.3 describes the three methods used to confirm that an invalid signal is marked with a faulty status: (1) Sensor maintenance; (2) PS detection of sensor failures; or (3) communication failure between PS computers. The staff finds that the reactor trip voting logic meets the single-failure criteria, since the voting modification scheme is able to accommodate a single failure so that the modified voting logic is able to issue an actuation order.

Based on the level of redundancy, independence, and FMEA, the staff finds that the PS design adequately addresses the single failure aspect of GDC 21 and guidance of RG 1.53, and that FSAR Tier 1, Section 2.4.1, ITAAC Item 4.18, provides a means to verify this design requirement. Therefore, the staff concludes that the PS meets the requirements of GDC 21 and IEEE Std 603-1998, Clause 5.1.

#### *7.1.4.5.3 SAS Single Failure Protection*

FSAR Tier 2, Section 7.1.1.4.2, "Safety Automation System," states that SAS performs automatic and manual grouped control functions to perform safety-related controls during normal operations, to mitigate the effects of AOOs and PAs, and to achieve and maintain safe shutdowns. The SAS is organized into four independent divisions. FSAR Tier 1, Section 2.4.4, "Safety Automation System," states that the SAS is designed so that safety-related functions required for AOOs or PAs are performed in the presence of the single detectable failures within SAS concurrent with identifiable but non-detectable failures, failures caused by the single failure, and failures and spurious system actions that cause, or are caused by, the AOO or PA requiring the safety function.

The applicant changed SAS functionality from 2nd min/2nd max to a sensor/setpoint comparison scheme. The change is reflected in Interim Revision 3 mark-ups of FSAR Tier 2, Section 7.3, "Engineered Safety Features Systems." The change in SAS from 2nd min/2nd max to a voting scheme is only reflected on FSAR Tier 2, Figures 7.3-4, "EFWS SG Level Control and Pump Flow Protection," and 7.3-12, "MSRCV Control." The change in design functionality can be found in FSAR Tier 2, Section 7.3, Figure 7.3-12, Interim Revision 3 mark-ups. The staff did not identify design detail on SAS voting and how voting logic is changed in the presence of faulty signals (single failures) within the FSAR. The FSAR also does not provide any details on what would be considered a "typical actuation logic sequence" such as in FSAR Tier 2, Section 7.3, Figure 7.3-1, "Typical ESF Actuation," Sheets 1 and 2.

The SAS is in continuous operation. Secondly, in terms of accident mitigation, the SAS does not actuate on its own. The portions of SAS that support accident mitigation are only initialized when instructed to do so by the PS, and only for a specific set of ESF actuations. Instead of utilizing APUs and ALUs like the PS, SAS utilizes control units (CUs). FSAR Tier 2, Section 7.1.1.4.2 states that the CUs execute the logic for the SAS automatic and manual grouped control functions. The SAS component configuration and operational features are significantly different from the PS. The applicant also states the following concerning CUs in FSAR Tier 2, Section 7.1.1.4.2:

Multiple sets of redundant CUs may be used, depending on sizing requirements. Redundant CUs in multiple divisions may have interdivisional communications between them to perform their functions.

The staff finds the statement ambiguous. FSAR Tier 2, Figure 7.1-7, "Safety Automation System Architecture," shows that the SAS is a four-division system and clearly shows interdivisional communication between CUs. Based upon the above quoted statement, the configuration shown in FSAR Tier 2, Figure 7.1-7 is not definitive and is subject to change. Additional information is needed in the FSAR concerning SAS logic, voting, and actuation to permit the staff to make a reasonable assurance finding as required by 10 CFR 52.47(a)(2). The staff determined that the requirements of IEEE Std 603-1998, Clause 5.1 have not been met for this aspect of SAS, because it is unknown how SAS voting logic compensates for single failures within a SAS division. Therefore, in RAI 505, Question 07.01-36, the staff requested that the applicant provide more details on the new SAS voting configuration and document this information in FSAR. The staff also requested that the applicant provide a definitive statement in FSAR regarding SAS logic configuration. **RAI 505, Question 07.01-36 is being tracked as an open item.**

Similar to the PS architecture, the staff noted that the SAS architecture has several interconnections that could affect single failure protection. Unlike the PS, the staff could not identify a single failure analysis, such as an FMEA, that demonstrated single failure protection of the SAS. Therefore, in RAI 505, Question 07.01-35, the staff requested that the applicant provide an FMEA, or similar single failure analysis, for the SAS. In addition, the staff requested that the applicant provide an ITAAC to verify the SAS single failure analysis, similar to the PS ITAAC to verify its FMEA. **RAI 505, Question 07.01-35 is being tracked as an open item.**

#### *7.1.4.5.4 PACS Single Failure Protection*

The staff reviewed the single-failure protection characteristics of the PACS against requirements in IEEE Std 603-1998, Clause 5.1, "Single Failure Criterion," and 10 CFR Part 50, Appendix A, GDC 21. The staff used the guidance in RG 1.53, which endorses IEEE Std 379-2000, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

FSAR Tier 2, Sections 7.1.1.6.3, "Redundancy," and 7.1.1.6.4, "Independence," address single failure protection. The applicant states, in part, that redundancy is implemented throughout the I&C architecture to prevent a single failure from causing a loss of function. The level of redundancy assigned depends on the classification and functional requirements of the system. There are four levels of redundancy for the PACS. In addition, for safety I&C systems, independence is established so that a single failure does not result in the loss of the safety function. The applicant also performed a system level failure modes and effects analysis to verify conformance with the single failure criterion. The analysis is described in FSAR Tier 2, Section 7.3.2.2, "Failure Modes and Effects Analysis," and the results are summarized in Technical Report ANP-10309P, Appendix A, Table A.3-1, "FMEA Results Table." The analysis shows that the chosen hardware, architecture, and implementation of the module sufficiently controls all postulated failure modes to prevent unallowable failures within the module. Therefore, the staff finds that the PACS design meets the requirements of Clause 5.1 of IEEE Std 603-1998 and GDC 21.

#### *7.1.4.5.5 ICIS Single Failure Protection*

FSAR Tier 2, Section 7.1 states, in part, that the ICIS cabinets are organized into four divisions and send 72 SPND output signals and 36 COT signals to the SCDS for distribution to the DCS through electrically isolated, hardwired connections. As described in Section 7.1.4.1 of this report, the applicant requested an alternative to IEEE Std 603-1991, Clause 5.6.1 with regards to independence. As described in Section 7.1.4.1 of this report, while the ICIS does not meet the independence requirements, it does provide for single failure protection. Specifically, a single failure of an SPND or its signal conditioning circuitry to the signal multiplier/isolator would not prevent the safety function as the safety analysis already considers a worst-case single failure of an SPND or its signal conditioning circuitry. Section 7.1.4.1 of this report discusses compliance of the ICIS to IEEE Std 603-1998, Clause 5.1 and GDC 21.

#### *7.1.4.5.6 EIS Single Failure Protection*

FSAR Tier 1, Section 2.4.17, "Excore Instrumentation System," states that the EIS provides signals indicative of neutron flux level conditions to the SCDS. In FSAR Tier 1, Table 2.4.17-1, "Excore Instrumentation System Equipment," the applicant states that three Source Range Detectors are routed to three divisions, four intermediate range detectors are routed to the four independent divisions, and four sets of upper core half and lower core half power range detectors are routed to the four independent divisions. These detectors are located in the reactor building, but information is routed to the respective divisions. The EIS cabinets are organized into four redundant divisions and send intermediate range and power range detector signals to the SCDS for distribution to the DCS through electrically isolated, hardwired connections.

FSAR Tier 2, Table 7.1-2, Sheet 3 of 9, lists the EIS as one of the safety I&C systems that is designed to meet GDC 21. FSAR Tier 2, Table 7.1-2, Sheet 5 of 9, lists the EIS as one of the safety I&C systems that is designed to conform to RG 1.53. Based on Tier 1 information, there is an adequate level of redundancy and independence since each division receives signals from its respective IRDs and PRDs. IRDs and PRDs provide inputs to PS through SCDS. Based on the PS FMEA in Technical Report ANP-10309P, the PS voting logic is modified to accommodate a single-failure of any detector. Therefore EIS can handle a single failure and still perform its intended safety function, which is to provide neutron flux level signals to the SCDS.

Based on this level of redundancy and independence, the staff finds that the EIS design meets the single failure aspect of IEEE Std 603-1998, Clause 5.1 and GDC 21.

#### *7.1.4.5.7 BCMS Single Failure Protection*

FSAR Tier 1, Section 2.4.11, "Boron Concentration Measurement System," states that the BCMS measures the boron concentration in the chemical and volume control system, and sends the boron concentration measurement signals to the SCDS in the four independent divisions. The applicant also states that there are four boron concentration and temperature sensors located in the Fuel Building, which are routed to the four independent divisions, and the four BCMS cabinets are located in their respective four Safeguard Buildings.

FSAR Tier 2, Table 7.1-2, Sheet 3 of 9, lists the BCMS as one of the safety-related I&C systems that is designed to meet GDC 21. FSAR Tier 2, Table 7.1-2, Sheet 5 of 9, lists the BCMS as one of the safety-related I&C systems that is designed to conform to RG 1.53. TS Table 3.3.1-1 (Page 1 of 6), Component 2, Boron Concentration – Chemical and Volume Control System

Charging Line sensors, states that three out of four is the minimum required for functional capability. This means that the BCMS can handle a single sensor failure and still perform its intended safety function.

Based on the level of redundancy and independence, the staff finds that the BCMS design meets the requirements of IEEE Std 603-1998, Clause 5.1 and GDC 21.

#### *7.1.4.5.8 RMS Single Failure Protection*

FSAR Tier 1, Section 2.4.22, "Radiation Monitoring System," states that the RMS provides surveillance of ionizing radiation comprising all provisions dealing with the occurrence of ionizing radiation within the plant and measures related to the health control of personnel who could be exposed to radiation. The RMS provides radiation measurement output signals to the SCDS from the containment high range dose rate monitor and from the main steam line radiation monitor. FSAR Tier 1, Table 2.4.22-1, "Radiation Monitoring System Equipment Mechanical Design," states that there are four containment high range dose rate monitors in the reactor building, four main steam line radiation monitors located in the main steam valve room which are routed to the four independent divisions, and four radiation monitoring cabinets located in each of the four safeguard buildings. FSAR Tier 2, Table 7.1-2, Sheet 3 of 9, lists the RMS as one of the safety-related I&C systems that is designed to meet GDC 21. FSAR Tier 2, Table 7.1-2, Sheet 5 of 9, lists the RMS as one of the safety-related I&C systems that is designed to conform to RG 1.53. Based on Tier 1 information, there is an adequate level of redundancy and independence since each SCDS division receives signals from its respective RMS division. Therefore, RMS can handle a single failure and still perform its intended safety function, which is to provide radiation measurements to the SCDS.

Based on this level of redundancy and independence, the staff finds that the RMS design meets the requirements of IEEE Std 603-1998, Clause 5.1 and GDC 21.

#### *7.1.4.5.9 HMS Single Failure Protection*

FSAR Tier 1, Section 2.4.14, "Hydrogen Monitoring System," states that HMS provides for the monitoring of hydrogen concentration in the containment atmosphere. FSAR Tier 2, Section 6.2.5.2.2, "Hydrogen Monitoring System," states that there are two subsystems of the HMS that measure hydrogen concentrations within containment: (1) The low range system measures hydrogen concentrations during design basis events, and (2) the high range system measures hydrogen and steam concentrations during and after beyond design basis events. The applicant states that hydrogen concentrations are measured continuously during plant operation and are available for display in the main control room. The low range HMS signal processing unit is located in Safeguard Building 1 and is powered from Class 1E electrical power supply. Also, the loss of a measuring channel or failure of the signal processing unit is indicated. FSAR Tier 2, Section 6.2.5.3, "Safety Evaluation," states that the low range HMS meets the single failure criterion, because its sensors are located in seven physically separated areas of the containment and the failure of one sensor does not influence the reliability or accuracy of the remaining sensors.

FSAR Tier 2, Section 6.2.5.3 states that the high range HMS system consists of two redundant trains of gas samplers and the associated piping running to the process and analysis modules. The high range HMS equipments is located in Safeguard Buildings 1 and 4 and is powered by the severe accident uninterruptible power supply. After the operator starts the high range HMS manually, the system automatically cycles through the sampling points, and processes, analyzes, and displays the results in the main control room. FSAR Tier 2, Section 6.2.5.3.3



states that the high range HMS meets the single failure criterion in that there are redundant trains physically separated in different Safeguard Buildings. Each train is equipped with measuring points inside and outside the equipment rooms so that if a measuring unit is lost, the measurements can be substituted by a redundant train. FSAR Tier 2, Table 7.1-2, Sheet 5 of 9, lists the HMS as one of the safety-related I&C systems that is designed to conform to RG 1.53.

Based on this level of redundancy and independence, the staff finds that the HMS design meets Clause 5.1 of IEEE Std 603-1998 and GDC 21

#### *7.1.4.5.10 SCDS Single Failure Protection*

FSAR Tier 1, Section 2.4.25, states the SCDS provides signal conditioning and distribution of signals that it receives from Class 1E sensors or black boxes. The applicant also states that there is a SCDS cabinet located in each of the four independent divisions. FSAR Tier 2, Table 7.1-2, Sheet 3 of 9, lists the SCDS as one of the safety-related I&C system that is designed to meet GDC 21. FSAR Tier 2, Table 7.1-2, Sheet 5 of 9, lists the SCDS as one of the safety-related I&C system that is designed to conform to RG 1.53. FSAR Tier 2, Table 7.1-1 states that the SCDS I&C system has a level of redundancy of four.

Based on this level of redundancy and independence, the staff finds that the SCDS design meets the requirements of IEEE Std 603-1998, Clause 5.1 and GDC 21.

#### *7.1.4.5.11 RPMS Single Failure Protection*

FSAR Tier 1, Revision 3, Section 2.4.26, "Rod Position Measurement System," states that the rod position measurement system measures the position of a rod control cluster assembly located within the reactor vessel, and it provides the measurement to the DCS. The applicant also states that there is a RPMS equipment cabinet located in each of the four independent divisions. FSAR Tier 2, Table 7.1-2, Sheet 3 of 9, lists the RPMS as one of the safety-related I&C system that is designed to meet GDC 21. Since all RPMS signals go to four independent divisions, the RPMS system is redundant.

Based on this level of redundancy and independence, the staff finds that the RPMS design meets the requirements of IEEE Std 603-1998, Clause 5.1 and GDC 21.

#### *7.1.4.6 Completion of Protective Action*

The staff reviewed the U.S EPR application to determine if IEEE Std 603-1998, Clause 5.2 has been adequately addressed for the EPR safety systems. IEEE Std 603-1998, Clause 5.2 requires the U.S. EPR safety system design to provide features to ensure that system-level actions go to completion. Per the guidance in SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," the staff review of this item included a review of the functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion. FSAR Tier 2, Section 7.1.2.6.13, states that the safety systems meet the requirements of IEEE Std 603-1998, Clause 5.2, in that, when initiated by the safety system, protective actions proceed to completion, and a return to normal operation requires deliberate operator intervention.

IEEE Std 603-1998, Clause 7.3 requires, in part, the design of the execute features such that, once initiated, the protective action of the execute features goes to completion. FSAR Tier 2, Section 7.1.2.6.13, "Completion of Protective Action (Clauses 5.2 and 7.3)," states that the

execute features are designed so that once initiated, the protective actions continue until completion, in accordance with IEEE Std 603-1998, Clause 7.3.

#### *7.1.4.6.1 PS and Completion of Protective Action*

The ESF I&C functions are described in FSAR Tier 2, Section 7.3.2, "Analysis." In this section, the applicant states that once an ESF function is actuated, it will proceed to completion and require operator intervention to return ESF actuators to a normal state. The applicant also states that in cases where the removal of a demand signal from an associated PACS module could result in a change in state of the actuator (i.e., solenoid operators), then seal-in logic is incorporated into the execute features. The seal-in features allow for the removal of the demand signal while still requiring deliberate manual action to change the state of the affected actuator(s). The ITAAC for this design aspect of ESF is discussed in FSAR Tier 1, Section 2.4. However, the ITAAC in FSAR Tier 1, Table 2.4.1-7, "Protection System ITAAC," did not test for this criterion to verify system design. Therefore, in RAI 59, Question 07.03-09, the staff requested that the applicant provide an ITAAC to verify completion of protective action. The applicant provided the response to this RAI as part of a response to a Chapter 9 RAI. In a June 12, 2009, response to RAI 60, Question 09.03-09, the applicant provided an ITAAC Map. With this map, the applicant identified where IEEE Std 603-1998 clauses are addressed in the ITAAC. The staff reviewed the applicant's response and finds the applicant meets the requirements of IEEE Std 603-1998, Clauses 5.2 and 7.3. Additionally, ITAAC FSAR Tier 1, Table 2.4.1-7, Items 4.1 and 4.2 provide ITAAC that verifies completion of protective action for both RT and ESF functions. Therefore, the staff concludes that the U.S. EPR design meets IEEE Std 603-1998, Clauses 5.2 and 7 and 10 CFR 52.47(b)(1) for this design aspect.

#### *7.1.4.6.2 SAS and Completion of Protective Action*

SAS is a Class 1E system that provides controls that include safety-related interlocks and helps the plant achieve and maintain safe shutdown conditions. During the initial review, the staff did not find an ITAAC item in FSAR Tier 1, Revision 3 Table 2.4.4-6, "Safety Automation System ITAAC," that verifies the requirements of IEEE Std 603-1998, Clauses 5.2 and 7.3 have been incorporated into the SAS design. There is insufficient technical information on SAS architecture or logic configuration available in FSAR for the staff to determine how the requirements of IEEE Std 603-1998, Clause 5.2 and Clause 7.3 can be implemented.

In a June 12, 2009, response to RAI 78, Question 14.03.05-4, the applicant provided the following explanation in a note concerning SAS compliance:

Completion of protective action is verified by several ITAAC. ITAAC Item 4.2 in Section 2.4.1 verifies that an ESF actuation signal remains as long as conditions that represent the completion of the function do not exist and requires deliberate operator action to be returned to normal. ITAAC Item 4.4 in Section 2.4.5 verifies proper connections from the other I&C systems to the PACS. Various mechanical system PACS ITAAC are provided that verify that the actuator responds to the state requested by the test signal sent to the PACS. Examples of this ITAAC can be found in FSAR Tier 1, Sections 2.2.1, 2.2.3, 2.2.4, 2.2.7, 2.6.1, 2.6.6, 2.7.1, 2.7.2, 2.7.11. All ITAAC items mentioned above provide verification that completion of protective action requirement is satisfied.

In addition to the above statement, ITAAC Item 4.18 verifies all the automatic functions of SAS listed in FSAR Tier 1, Table 2.4.4-5, "Safety Automation System ITAAC."

In RAI 505, Question 07.01-37, the staff requested that the applicant add an ITAAC item to FSAR Tier 1, Section 2.4.5, "Priority and Actuator Control System," that would link the testing done with SAS-related mechanical system PACS testing to ITAAC Item 4.4 in FSAR Tier 1, Section 2.4.5 to ensure that the SAS ITAAC contains sufficient information to ensure IEEE Std 603-1998 Clause 5.2 and 7.3 are addressed, and that completion of the SAS ITAAC is tied to the various mechanical system PACS ITAAC being completed satisfactorily. **RAI 505, Question 07.01-37 is being tracked as an open item.**

#### *7.1.4.6.3 PACS and Completion of Protective Action*

The staff was initially unable to locate specific information regarding completion of protective action for the PACS in the applicant's submittals for FSAR. The applicant indicated that there is no functionality in the PACS for completion of protective action. In RAI 373, Question 07.01-22, the staff requested that the applicant describe how the PACS meets IEEE Std 603-1998, Clause 5.2. In an August 13, 2010 response to RAI 373, Question 07.01-22, the applicant stated that the PS upstream of the PACS, and electrical switchgear downstream of the PACS provide for the completion of protective actions, which is specifically addressed in FSAR Tier 2, Section 7.1.2.6.13. The staff finds the applicant's response is acceptable, since the PS and electrical switchgear would ensure the completion of protective action and the PACS only responds to signals from those systems and components. FSAR Tier 1, Section 2.4.1, ITAAC Item 4.2 provides an acceptable verification of completion of protection action for the safety functions. Therefore, the staff finds that the PACS design meets the requirements of IEEE Std 603-1998, Clauses 5.2 and 7.3 and 10 CFR 52.47(b)(1).

#### *7.1.4.7 Quality*

The staff reviewed the U.S. EPR design to determine if the quality standards requirements of GDC 1 were adequately addressed. This discussion is located in Section 7.1.4.3 of this report. Additionally, the staff reviewed the application to determine if IEEE Std 603-1998, Clause 5.3 has been adequately addressed. IEEE Std 603-1998, Clause 5.3 requires that components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. GDC 1 requires, in part, a quality assurance program be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. The staff used the guidance in SRP Appendix 7.1-C. The review guidance provided in SRP Appendix 7.1-C, Subsection 5.3, "Quality," indicates that the application should confirm that the quality assurance provision of 10 CFR Part 50, Appendix B is applicable to the safety system.

FSAR Tier 2, Section 7.1.2.6.14, "Quality (Clause 5.3)," states that the safety systems meet the requirements of IEEE Std 603-1998, Clause 5.3 and that the safety systems are within the scope of the U.S. EPR quality assurance program, which is described in FSAR Tier 2, Section 17.5, "Quality Assurance Program Description." FSAR Tier 2, Section 17.5, states that the quality assurance plan for the U.S. EPR was approved by the staff. The staff approval is documented the safety evaluation report for in Topical Report ANP-10266A, "AREVA NP Inc. Quality Assurance Plan for the U.S. EPR Topical Report," Revision 1, FSAR Tier 2, Section 7.1.2.6.14 also states that the TXS hardware quality is described in Topical Report EMF-2110(NP)(A), Revision 1. FSAR Tier 2, Section 7.2.2.3.2, "Compliance to Requirements for Quality of Components and Modules (Clause 5.3 of IEEE Std 603-1998 and Clause 5.3 of IEEE 7-4.3.2-2003)," states that components and modules that are required to perform the

reactor trip function are classified as safety-related and are designed in accordance with a quality assurance program. Additionally, FSAR Tier 2, Section 7.3.2.3.2, states that protection system components and modules that are required to perform ESF actuation functions are classified as safety-related, are designed to Class 1E standards, and are applied in accordance with a quality assurance program.

U.S. EPR compliance to IEEE Std 603-1998, Clause 5.3 is stated in FSAR Tier 2, Sections 7.1.2.6.14, 7.2.2.3.2, and 7.3.2.3.2. In each section, the applicant states that the PS components are designed to Class 1E standards in accordance with guidance from IEEE Std 603-1998 and IEEE Std 7 4.3.2-2003. The TXS system software was developed in accordance with the process described in Topical Report EMF-2110. The verification and validation (V&V) of the application software will be performed in accordance with Topical Report ANP-10272. Based upon this and the quality assurance program described in Topical Reports ANP-10266A and EMF-2110 and Technical Report ANP-10272, the staff finds the U.S. EPR safety-related I&C systems meet the requirements of IEEE Std 603-1998, Clause 5.3. and GDC 1

#### *7.1.4.7.1 PACS Quality*

FSAR Tier 2, Section 7.1.1.4.3, "Priority and Actuator Control System," states that the PACS is designed under the TXS quality assurance program, which was previously reviewed and approved by the staff. The staff finds the quality commitment for the PACS acceptable.

Digital I&C Interim Staff Guidance (DI&C ISG)-04, "Highly Integrated Control Room – Communications," Section 2 states, in part, that existing diversity and defense-in-depth guidance indicates that diverse actuation signals should be applied to plant equipment control circuits downstream of the digital system to which they are diverse, in order to ensure that the diverse actuation will be unaffected by digital system failures and malfunctions. Accordingly, the priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to SCCF. Adequate configuration control measures should be in place to ensure that software-based priority modules that might be subject to SCCF will not be used for credited diversity. The applicant should demonstrate that such measures are in place, those provisions fit into the overall 10 CFR Part 50, Appendix B, quality assurance program, and that the priority module meets all of the 10 CFR Part 50, Appendix A and B quality requirements (design, qualification, quality, etc.) applicable to safety-related hardware or software.

DI&C ISG-04, Section 2 further states that the priority module itself should be shown to apply the commands correctly in order of their priority rankings and that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis. In addition, validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100 percent tested before being released for service. One hundred percent testing means that every possible combination of inputs and every possible sequence of device states is tested and all outputs are verified for every case. The testing should not involve the use of the design tool itself.

The applicant submitted Technical Report ANP-10310, "Methodology for 100% Combinatorial Testing of the U.S. EPRTM Priority Module Technical Report," Revision 1, to demonstrate adequate software quality of the PACS module through 100 percent combinatorial testing. Technical Report ANP-10310P presents an illustrative example of the methodology for the 100 percent combinatorial testing of an SPLM1-PC10 priority module. The priority module for

U.S. EPR will have a level of complexity no greater than the SPLM1-PC10 module presented in the example.

The safety-related portion of PACS utilizes an electronic module where the logic functions performing priority control and command termination are implemented by using programmable logic devices (PLDs). Adaptation between the module internal signal levels to the external signal levels and module internal functionality are implemented using discrete electronics. Some self-monitoring features may also be implemented in the PLD.

### Input Signals and Internal States

Technical Report ANP-10310P, Section 4.0 provides a description of the 100 percent combinatorial testing. The priority logic implemented in the PACS is predominantly combinatory logic, but state-based logic is also included. The input signals are actuation signals of varying types, including non-latched actuation signals, latched actuation signals, delayed actuation signals, and infrastructure signals. These signals bound the possible functionality of the priority module, but may not all be used in the as-built priority module. Additionally, each input that can affect the output of a priority module is tested individually by applying a series of input signals of varying durations to account for the possibility of invalid signals.

During testing all possible combinations of actuation signals are applied as inputs to the priority module with infrastructure signals maintained at values indicating that all support elements are functioning normally. The resulting outputs are compared to the expected outputs for every combination. Non-latched signals are not used in a state-based manner. Therefore, each possible combination of non-latched actuation signals is tested, with no requirement on the combination test sequence. Latched actuation signals and delayed actuation signals are state based. Therefore, in the definition of all possible combinations of actuation signals, these signals must be applied in specific manner such that the sequences of input sets where the output can depend on a previous input set are tested and timing variances are accounted for. The outputs are then compared to the expected outputs, for every combination of inputs.

Infrastructure signals are signals received by the priority module that indicate the status of hardware elements that support the priority module (e.g., power supply status, output driver status, specific test modes). An infrastructure signal does not request an action of the final actuated device. It is used to set the output of the priority module to a predefined value in case of a fault in a hardware element supporting the priority module. These signals are generated based only on signals originating in the module or the module's division. Infrastructure signals are not required to be included in the definition of all possible combinations of valid actuation signals, because the inputs are unique to each division of the PACS (i.e., there is no common external stimulus between the redundant divisions). Therefore, infrastructure signals would not induce a common cause failure (CCF).

### Automatic Testing

DI&C ISG-04, Section 2.0, Point 8 states, in part, that the priority module design should be fully tested (proof-of-design testing) to minimize the probability of failures due to common software. Testing should include the application of every possible combination of inputs, including internal states, and the evaluation of all resulting outputs. If the tests are generated by any automatic test generation program, then all the test sequences and test results should be manually verified.

Proof-of-design testing for the PACS priority module is implemented using an automatic test machine, which generates each combination of inputs to be tested, derives the expected outputs, inserts the combination of inputs into the priority module, identifies output discrepancies, and generates test logs. Technical Report ANP-10310P, Section 6.0 provides an example of the approach for implementation of the 100 percent combinatorial test methodology for the PACS using the SPLM1-PC10. It describes the hardware configuration and interconnections between the two primary PLDs in the module, Subsystems A and B. The technical report asserts that these are two separate devices and, therefore, combinatorial testing can be applied separately. Technical Report ANP-10310P, Figures 5-2 and 5-3 show that outputs of each subsystem may provide an external hardwired input to the other. Such an input is not complex or programmable and configuration control will be addressed through the quality assurance program. Technical Report ANP-10310P, Section 5.3 states that although the devices operate independently, both are needed to perform the complete priority function.

Technical Report ANP-10310P, Revision 0, Section 6.2 states, in part, that the internal states specified for SPLM1-PC10 functionality have a very direct effect on the module outputs. Accordingly, the effect of these internal states is easily observed at the module outputs. However, additional test outputs may be provided that allow complementary checking of the behavior of the internal states. DI&C ISG-04 states, in part, that 100 percent combination testing means that every possible combination of inputs and every possible sequence of device states is tested and all outputs are verified for every case and sequence of device states must be tested. The applicant did not provide a firm commitment that all internal states are observable and will be tested as a part of the test case in Technical Report ANP-10310P, Revision 0. Therefore, in RAI 373, Question 07.01-23, the staff requested that the applicant address the above commitment. In a December 3, 2010, response to RAI 373, Question 07.01-23, the applicant stated that internal states are directly observable for the purpose of testing, and will be included as outputs monitored in the 100 percent combinatorial testing of the module. The staff finds this RAI response is acceptable. The staff also notes that the above commitment was incorporated in the revised Technical Report ANP-10310P, Revision 1.

## Manual Verification

DI&C ISG-04, Section 2, Point 8, states that if the tests are generated by any automatic test generation program, then all the test sequences and test results should be manually verified. Technical Report ANP-10310P, Revision 0, Section 7.1 described the applicant's approach for manual verification of testing results generated by the automatic test generation program. The verifier first completes a basic check of the test machine log to ensure that the test machine performed all test cases and checks that the test case results are compliant with the main functions of the priority logic and to confirm that all tests are executed without error. The verifier then checks the test cases against the principles of the priority logic. In this step, the manual verification defines the expected outputs of the priority logic, which refers to only the command outputs sent to the actuated device, for every input signal combination. The methodology for manual verification describes a rule-based sorting of a subset of test cases involving priority logic only. The description of the sorting appeared inconsistent with the applicant's commitment to manually verify all test sequences and test results. In RAI 373, Question 07.01-24, the staff requested that the applicant clarify the rule-based sorting and 100 percent manual verification. In a December 3, 2010 response to RAI 373, Question 07.01-24, the applicant stated that the approach included in Technical Report ANP-10310P does provide 100 percent manual verification and that the sorting does not impact the ability to manually verify each test case. In summary, the applicant will manually verify all outputs of the priority module that are used for

safety-related functions for all test cases. The staff finds the applicant's response acceptable. In addition, the applicant included necessary changes in Technical Report ANP-10310P, Revision 1, which the staff also finds acceptable.

Overall, the staff finds that the PACS logic development using 100 percent combinatorial testing satisfies the guidance in DI&C ISG-04 and, therefore, meets the requirements of IEEE Std 603-1998, Clause 5.3.

#### *7.1.4.7.2 Software Quality*

To determine the acceptability of the applicant's software quality, the staff used the guidance in SRP Appendix 7.1-C and in SRP Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2." The guidance in SRP Appendix 7.1-C states that for digital computer-based systems, the staff is to confirm that the application addresses the quality requirements described in IEEE Std 7-4.3.2-2003, Clause 5.3 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." The guidance in SRP Appendix 7.1-D, Subsection 5.3 indicates that the application should address the quality criteria described in IEEE Std 7-4.3.2-2003, Clause 5.3 and that software quality is addressed in IEEE/Electronic Industries Alliance (EIA) Std 12207.0-1996, "Standard for Information Technology – Software Life Cycle Processes." IEEE Std 7-4.3.2-2003, Clause 5.3 indicates that the review of software quality also includes a review of software development, V&V, as well as independent V&V, software configuration management, and software project risk management. Also, SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," refers to IEEE Std 7-4.3.2-2003, Clause 5.3. SRP BTP 7-14 describes the specific features of software development that should be reviewed by the staff.

FSAR Tier 2, Section 7.1.2.6.14, states that its digital safety systems meet IEEE Std 7-4.3.2-2003 and the TXS system software is developed in accordance with the process described in Topical Report EMF-2110. Additionally, FSAR Tier 2, Section 7.1.2.6.14, states that the application software of the digital safety systems conforms to the guidance of IEEE Std 7-4.3.2-2003 with two exceptions: (1) Alternate V&V methods are used; and (2) configuration control board is not used. This one exception is discussed in Topical Report ANP-10272. Additional staff discussion on software quality is provided in the staff's review of Topical Report ANP-10272.

The staff finds that the U.S. EPR safety-related software development process meets the requirements of IEEE Std 603-1998, Clause 5.3, with the following exceptions. While the staff has completed its review of Topical Report ANP-10272, the applicant needs to incorporate by reference the approved version of the topical report. In addition, the applicant is requested to address the application-specific action items within the topical report. Therefore in RAI 505, Question 07.01-50, the staff requested that the applicant address the need for an approved version of Topical Report ANP-10272 and clarify how the U.S. EPR design addresses the application-specific action items within that topical report. **RAI 505, Question 07.01-50 is being tracked as an open item.**

#### *7.1.4.8 Equipment Qualification*

The staff reviewed the U.S. EPR design certification application to verify that GDC 2, "Design Bases for Protection Against Natural Phenomena," GDC 4, "Environmental and Dynamic Effects Design Bases," and IEEE Std 603-1998, Clause 5.4 have been adequately addressed for the U.S. EPR safety systems. GDC 2 requires, in part, that structures, systems, and components

important to safety shall be designed to withstand the effects of natural phenomena, such as earthquakes, tornadoes, hurricanes, floods, tsunamis, and seiches, without loss of capability to perform their safety functions. GDC 4 requires, in part, structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. IEEE Std 603-1998, Clause 5.4, requires, in part, that safety system equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of continually meeting the performance requirements, as specified in the design basis. The staff used the guidance of SRP Appendix 7.1-A, which indicates that the applicant's design bases should identify those systems and components that are qualified to accommodate the effects of environmental conditions. Also, the staff review included review of equipment qualification for environmental conditions in accordance with the guidance provided in SRP Appendix 7.1-C, Section 5.4, and SRP Appendix 7.1-D. Furthermore, regarding the staff determination of whether the design meets the requirements of GDC 4, the staff review of the application's equipment qualification for environmental conditions is conducted in accordance with the guidance in SRP Appendix 7.1-C, Section 5.4. Evaluation of conformance to IEEE Std 603-1998, Clause 5.4 is primarily addressed in the evaluation of conformance to IEEE Std 7-4.3.2-2003, Section 5.4.

The staff reviewed FSAR Tier 2, Section 7.1.2.2.2, "GDC 2 Design Bases for Protection against Natural Phenomena, and Section 7.1.2.2.3, "GDC – Environmental and Dynamic Effect of Design Bases." FSAR Tier 2, Section 7.1.2.2.2, states that compliance with IEEE Std 603-1998, Clause 5.4, demonstrates that the applicable I&C systems remain operable during and following seismic events (the applicable systems are identified in FSAR Tier 2, Table 7.1-2, as the SICS, PS, SAS, PACS, CRDCS, ICIS, EIS, BCMS, RMS, HMS, RPLVMS, RPMS, and SCDS). FSAR Section 7.1.2.2.3, states that compliance with IEEE Std 603-1998, Clause 5.4, demonstrates that the requirements of GDC 4 are met.

The staff reviewed FSAR Tier 2, Section 7.1.2.6.15, "Equipment Qualification (Clause 5.4)," and other applicable sections to verify that IEEE Std 603-1998, Clause 5.4, has been appropriately addressed. FSAR Tier 2, Section 7.1.2.6.15, states that the safety-related systems meet the requirements of IEEE Std 603-1998, Clause 5.4. FSAR Tier 2, Section 7.1.2.6.15 further states that the digital safety-related systems meet the additional guidance of IEEE Std 7-4.3.2-2003, and that integrated system testing including factory acceptance testing and site acceptance testing is performed as part of the TXS development process described in FSAR Tier 2, Section 7.1.1.2. FSAR Tier 2, Section 7.1.1.2, "Use of TELEPERM XS indicates the use of the principles and methods described in Topical Report EMF-2110. FSAR Tier 2, Section 7.1.1.2 includes a subsection, Section 7.1.1.2.1, "TXS Platform Design," which states in part, that the TXS lifecycle processes used for safety-related applications includes basic design, which consists of system requirements, system design, software requirements, detailed design, and system integration and testing. Additionally, the discussion of the staff review of the applicant's Environmental Qualification Program, which addresses the environmental, seismic, and electromagnetic interference and radio frequency interference (EMI/RFI) qualification program for safety-related equipment, is located in Section 3 of this report.

FSAR Tier 2, Sections 7.1.2.4.17, "RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," and 7.1.2.4.19; "RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants," state that the applicable I&C systems shall be designed to meet the guidance of RG 1.180 and RG 1.204, (as stated above, for which the applicable systems are identified in FSAR Tier 2, Table 7.1-2, as



the SICS, PS, SAS, PACS, CRDCS, ICIS, EIS, BCMS, RMS, HMS, RPLVMS, RPMS, and SCDS). FSAR Tier 2, Section 7.1.2.4.9, "RG 1.151 – Instrument Sensing Lines," states that the applicable I&C systems shall be designed to meet the guidance of RG 1.151; for which the applicable systems are identified in FSAR Tier 2, Table 7.1-2, as PS, RCSL system, PAS, HMS, and SCDS. FSAR Tier 2, Section 7.1.2.4.20, "RG 1.209 – Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," states that the applicable I&C systems are designed to meet the guidance of the RG 1.209 for which the applicable systems are identified in FSAR Tier 2, Table 7.1-2, as SICS, PS, RPMS, and SAS.

The staff reviewed FSAR Tier 2, Section 7.1.2.6.15, and other applicable sections to verify if IEEE Std 603-1998, Clause 5.4, has been appropriately addressed in regard to the ITAAC addressing electrical grounding for PS equipment to ensure lightning protection. As indicated in SRP Section 7.1-C-8 and IEEE Std 7-4.3.2-2003, lightning protection should be addressed as part of the review of electromagnetic compatibility. The applicant indicated that there is a commitment to meet the guidelines in RG 1.204. The commitment includes conformance with electrical grounding standards. FSAR Tier 1, Table 2.5.8-1, "Lightning Protection and Grounding System ITAAC," contains the inspection and testing procedure for lightning protection and grounding.

Based on the design description and commitments in FSAR Tier 1 and FSAR Tier 2 as described above, the staff finds that the U.S. EPR design meets the requirements of GDC2, GDC 4, and IEEE Std 603-1998, Clause 5.4.

#### 7.1.4.9 *System Integrity*

The staff reviewed the U.S. EPR design certification application to verify that IEEE Std 603-1998, Clause 5.5 and GDC 23 have been adequately addressed for the U.S. EPR safety systems. IEEE Std 603-1998, Clause 5.5 requires that the safety system accomplishes its safety functions under the full range of applicable conditions enumerated in the design basis. A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the critical points of time identified as required by IEEE Std 603-1998, Clause 4j. GDC 23 requires that the protection system be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced. SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provides supplemental guidance on evaluating response time for digital computer-based systems, and discusses design constraints that allow greater confidence in the results analyses or prototype testing to determine real-time performance. Sections 7.9.4.1 and 7.3 of this report provide additional discussion of the staff review of how the applicant addresses response time testing, as well as discussion of the applicant's response to RAIs associated with response time testing.

IEEE Std 7-4.3.2-2003 indicates that design for computer system integrity and design for test and calibration should be addressed as part of safety system integrity. Evaluation of computer system hardware integrity should be included in the evaluation against the requirements of IEEE Std 603-1998. Computer system software integrity (including the effects of hardware-software interaction) should be demonstrated by the applicant's software safety analysis activities. SRP BTP 7-14, Subsections B3.1.9 and B3.2.1, describe the acceptable characteristics of software safety plans and analyses. The staff's review for system integrity is discussed in the subsections below. The staff's evaluation of how the data communications

system meets the requirements of IEEE Std 603-1998, Clause 5.5 is discussed in Section 7.9.4.1 of this report.

#### *7.1.4.9.1 PS Integrity*

SRP Appendix 7.1-D provides guidance for meeting IEEE 7-4.3.2-2003. Conformance to this design criterion is discussed in FSAR Tier 2, Section 7.1.2.6.16, "System Integrity (Clause 5.5)." SRP Appendix 7.1-C, Section 5.5 states, in part:

During either partial or full system initialization or shutdown after a loss of power, control output to the safety system actuators should fail to a predefined, preferred failure state. A system restart upon restoration of power should not automatically transfer the actuators out of the predefined failure state. Changes to the state of plant equipment from the predefined state following restart and re-initialization (other than changes in response to valid safety system signals) should be under the control of the operator in accordance with appropriate plant procedures.

The applicant states the following in Technical Report ANP-10309P, Revision 2, Appendix A, under "Loss of Power":

In case of loss of offsite power, each PS division is supplied with its own battery until the emergency diesel generators are started and connected to the EUPS. A single failure of a divisional battery could result in loss of power to a PS division. In that case, all function processors in the division shutdown (no data communication is sent from the division) and all outputs go to a "0" state. This results in opening that divisions RT devices (the tripped state), and no actuation of engineered safety features actuation system (ESFAS) components controlled by that division. The other 3 PS divisions remain capable of performing their protective functions. Upon restoration of power to a PS division, all function processors go through a reset and start-up self-test mode, during which the outputs remain in a "0" state. Upon successful completion of the start-up self-test, each function processor enters its normal cyclic operation mode. The RT outputs will transition from the "0" state (trip) to their normal "1" state (no-trip). This alone does not return the affected RT breaker to its normal state. Manual action is required locally (re-rack the breaker) to return to its closed position. Upon successful completion of the start-up self-test, when each function processor enters its normal cyclic operation mode, ESFAS outputs remain in their normal "0" state. If an AOO or PA is in progress during restoration of power, a change of state of the ESFAS outputs (to the actuate state) occur to respond to the event.

This information would also envelope the function of the PACS module for each ESF equipment actuator. In a June 12, 2009 response to RAI 78, Question 14.03.05-4, the applicant included an "ITAAC Mapping" scheme so that staff reviewers could more easily locate where the applicant discusses compliance with applicable regulations and standards. Also, the applicant provided Interim Revision 3 mark-ups of FSAR, which identified tests that demonstrate compliance with Clause 5.5. FSAR Tier 1, Table 2.4.1-7, ITAAC Item 4.10 provides verification that the PS equipment can perform its safety function when subjected to various environmental conditions.

The staff reviewed the applicant's June 12, 2009 response to RAI 78, Question 14.03.05-4, as well as design information presented in FSAR Tier 2, Section 7.1, and Technical Report ANP-

10309. The applicant's response to RAI 78, Question 14.03.05-4 included Table 14.03.05-1 that matched the individual requirements of IEEE Std. 603-1998 with the applicable ITAAC that verified the design's compliance with those individual requirements. According to Table 14.03.05-1, ITAAC Items 3.10 and 4.10 verified that the requirements of Clause 5.5 and GDC 23 have been incorporated into the PS design, which the staff reviewed and found acceptable. The staff finds the applicant adequately addressed design for computer integrity. Based on the available design information including information provided in the applicant's response to RAI 78, Question 14.03.05-4, the staff has reasonable assurance that upon loss of power, the PS (RT and ESF) will fail into predefined states such that the safety function is maintained. Therefore, the staff finds that the U.S. EPR design meets the requirements of GDC 23 and IEEE Std 603-1998, Clause 5.5. Calibration, testing, and self-testing of PS are discussed in Section 7.1.4.11 of this report.

#### *7.1.4.9.2 SAS Integrity*

FSAR Tier 2, Section 7.1.2.6.16, System Integrity (Clause 5.5)," addresses IEEE Std 603-1998, Clause 5.5. The applicant states that the PS implements a fail-safe design, but does not discuss system integrity for SAS. Therefore, in a June 12, 2009, response to RAI 78, Question 14.03.05-4, the applicant indicated that IEEE Std 603-1998, Clause 5.5 is verified by ITAAC Item 4.1, located in FSAR Tier 1, Section 2.4.4. However, the staff did not find complete information regarding system integrity of SAS. In follow-up RAI 505, Question 07.01-38, the staff requested that the applicant provide information in FSAR Tier 1 and FSAR Tier 2 concerning how the fail-safe design is incorporated into SAS. In particular, the staff requested that the applicant describe the behavior of SAS during a "loss of power" event, similar to the analysis provided in Technical Report ANP-10309P for the PS. **RAI 505, Question 07.01-38 is being tracked as an open item.**

#### *7.1.4.9.3 SICS Integrity*

FSAR Tier 2, Section 7.1.2.6.16, addresses compliance to IEEE Std 603-1998, Clause 5.5. The applicant states that the safety systems are designed to meet the requirements of IEEE Std 603-1998, Clause 5.5. However, Interim Revision 3 mark-ups of FSAR Tier 2, Section 7.1.2.6.16 do not discuss Clause 5.5 compliance for SICS. FSAR Tier 1, Section 2.4.2, states that the SICS can perform its safety function when subjected to electromagnetic interference (EMI), radio-frequency interference (RFI), electrostatic discharge (ESD), and power surges. FSAR Tier 1, Table 2.4.2-2 "Safety Information and Control System ITAAC," ITAAC Item 4.4 verifies this information. In RAI 505, Question 07.01-38, the staff requested that the applicant explain why the SICS was omitted from FSAR Tier 2, Section 7.1.2.6.16. The staff also requested that the applicant provide information on how the SICS recovers from a "loss of power" scenario and whether it is a "fail-safe" design. **RAI 505, Question 07.01-38 is being tracked as an open item.**

#### *7.1.4.9.4 PACS Integrity*

In FSAR Tier 2, Section 7.1.2.6.16, the applicant states that safety systems are designed to perform their functions as described in the design basis. Equipment qualification is performed so that the safety systems perform their function under the range of conditions required for operation. The PACS is implemented in four divisions located in physically separated Safeguard Buildings with electrical and communications independence measures. The applicant also states that the design for computer integrity, test and calibration, fault detection, and self-diagnostics provide for system integrity. The staff finds that PACS meets IEEE Std

603-1998, Clause 5.5 since its design provides for independence, equipment qualification, and test and calibration.

The applicant does not identify any self-testing features to credit for surveillance tests. This aspect of PACS design is further discussed in Section 7.1.4.11.5 of this report.

#### *7.1.4.9.5 Integrity of Other Safety I&C Systems*

FSAR Tier 2, Section 7.1.2.6.16, addresses compliance to IEEE Std 603-1998, Clause 5.5. The applicant states that the safety systems are designed to meet the requirements of IEEE Std 603-1998, Clause 5.5. During the course of the review, the staff did not find design information within FSAR Tier 2 regarding ICIS, EIS, BCMS, SCDS, RPMS, and RMS, with regard to how these systems recover from a loss-of-power condition. Specifically, if a loss-of-power situation for these individual systems occurs, the staff could not find design information in FSAR Tier 2 describing how system inputs and outputs would be affected and whether these systems have a predefined safe state that requires operator action to restore them to normal operating conditions. Therefore, in RAI 505, Question 07.01-38, the staff requested that the applicant provide information on how ICIS, EIS, BCMS, SCDS, RPMS, and RMS recover from a loss-of-power scenario, whether there is a fail-safe design, and how that design is implemented for each system. **RAI 505, Question 07.01-38 is being tracked as an open item.**

#### *7.1.4.10 Independence*

The staff reviewed the U.S. EPR design certification application to verify that the requirements of IEEE Std 603-1998, Clause 5.6, GDC 21, GDC 22, and GDC 24 have been adequately addressed for the U.S. EPR safety systems. GDC 21 requires redundancy and independence designed into the protection system to be sufficient to ensure no single failure results in a loss of the protection function and removal from service of any component or channel does not result in loss of the required minimum redundancy. GDC 22 requires the protection system be designed to assure the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function. GDC 24 requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or removal from service of any protection system component or channel common to control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. IEEE Std 603-1998, Clause 5.6 requires independence between (1) redundant portions of a safety system, (2) safety systems and effects of DBE, and (3) safety systems and other systems. NUREG-0800, Appendix 7.1-C, provides acceptance criteria for the requirements of IEEE Std 603-1998. NUREG-0800, Appendix 7.1-C, Section 5.6 states that three aspects of independence should be addressed, including physical independence, electrical independence, and communications independence. The staff also identified functional independence as an additional aspect that should be addressed. RG 1.75, "Criteria for Independence of Electrical Safety Systems," describes a method acceptable to the staff for complying with NRC regulations with respect to the physical independence requirements of the circuits and electrical equipment that comprise or are associated with safety systems. RG 1.75 endorses IEEE Std 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits," as an acceptable method for satisfying the regulatory requirement concerning physical independence of circuits and electrical equipment that comprise safety systems. SRP BTP 7-11, "Guidance on Application and Qualification of Isolation Devices," provides guidance on application and qualification of isolation devices used to ensure electrical independence for safety systems. In addition, Digital I&C ISG-04 (D I&C ISG-04), "Highly Integrated Control

Room – Communications,” Revision 1, provides design criteria for communication and functional independence between redundant divisions of safety systems.

#### *7.1.4.10.1 Independence Between Redundant Portions of the Safety System*

IEEE Std 603-1998, Clause 5.6.1, requires redundant portions of the safety system to be independent and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function. As stated above, RG 1.75 provides guidance on acceptable means to meet physical independence requirements.

##### **7.1.4.10.1.1 Physical Separation Between Redundant Portions of Safety Systems**

FSAR Tier 2, Section 7.1.1.6.4, Interim Revision 3 mark-ups, submitted as part of the June 22, 2011 response to RAI 442, Question 07.01-26 states that the PS, SAS, SCDS, and PACS each consists of four independent divisions. Physical separation is achieved by ensuring that the independent divisions are located in four physically separated Safeguard Buildings.

FSAR Tier 2, Section 7.1.2.4.5, “RG 1.75 – Criteria for Independence of Electrical Safety Systems,” states that applicable I&C systems listed in FSAR Tier 2, Table 7.1-2, shall be designed to meet the guidance of RG 1.75. The I&C systems in FSAR Tier 2, Table 7.1-2, that will be designed to meet the guidance of RG 1.75 include the SICS, SCDS, PS, SAS, PACS, CRDCS, ICIS, EIS, BCMS, RMS, HMS, RPLMS, and RPMS. FSAR Tier 2, Section 7.2.2.3.3, “Compliance to Requirements for Independence of the RT Function (Clauses 5.6 and 6.3 of IEEE Std 603-1998 and GDC 24),” states that the U.S. EPR design for the RT system maintains physical separation of redundant safety divisions throughout the systems extending from the sensors to the devices actuating the protection function. Separation of wiring is achieved using separate wire ways, cable trays, and containment penetrations for each division. Separate power feeds energize each redundant protection division. Cable separation and conformance to RG 1.75 is further discussed in FSAR Tier 2, Chapter 8, “Electric Power.”

The following ITAAC are provided in FSAR Tier 1, Interim Revision 3 mark-ups to verify that adequate physical separation exists between redundant portions of safety systems:

- FSAR Tier 1, Revision 3, Table 2.4.1-7, “Protection System ITAAC,” Item 2.2 verifies that physical separation exists between the four divisions of the PS. The acceptance criterion to verify this commitment is that the four divisions of the PS are located in separate Safeguard Buildings as listed in FSAR Tier 1, Revision 3, Table 2.4.1-1, “Protection System Equipment.”
- FSAR Tier 1, Revision 3, Table 2.4.2-2, “Safety Information and Control System ITAAC,” Item 2.5 verifies that physical separation exists between the Class 1E electrical divisions that power the controls and indications of the SICS. The acceptance criterion to verify this commitment is that the Class 1E electrical divisions that power the controls and indications of the SICS as listed in FSAR Tier 1, Revision 3, Table 2.4.2-1, “Safety Information and Control System Equipment,” are located in separate Safeguard Buildings.
- FSAR Tier 1, Revision 3, Table 2.4.4-6, “Safety Automation System ITAAC,” Item 2.2 verifies that physical separation exists between the four divisions of the SAS. The acceptance criterion to verify this commitment is that the four divisions of the SAS are located in separate Safeguard Buildings as listed in FSAR Tier 1, Table 2.4.4-1, “Safety Automation System Equipment.”

- FSAR Tier 1, Revision 3, Table 2.4.5-3, "Priority and Actuator Control System ITAAC," Item 2.2 verifies that physical separation exists between the four divisions of the PACS. The acceptance criterion to verify this commitment is that the four divisions of the PACS are located in separate Safeguard Buildings as listed in FSAR Tier 1, Revision 3 Table 2.4.5-1, "Priority and Actuator Control System Equipment."
- FSAR Tier 1, Revision 3, Table 2.4.25-4, "Signal Conditioning and Distribution System ITAAC," Item 2.2 verifies that physical separation exists between the four divisions of the SCDS. The acceptance criterion to verify this commitment is that the four divisions of the SCDS are located in separate Safeguard Buildings as listed in FSAR Tier 1, Table 2.4.25-1, "Signal Conditioning and Distribution Equipment."
- FSAR Tier 1, Revision 3, Table 2.4.26-4, "Rod Position Measurement System ITAAC," Item 2.2 verifies that physical separation exists between the four divisions of the RPMS. The acceptance criterion to verify this commitment is that the four divisions of the RPMS are located in separate Safeguard Buildings as listed in FSAR Tier 1, Revision 3, Table 2.4.26-1, "Rod Position Measurement System Equipment."

Based on the commitments to locate the independent divisions of the SCDS, PS, SAS, and PACS in separate Safeguard Buildings and to conform with RG 1.75 for adequate physical separation of these systems, the staff finds that sufficient physical separation between the redundant portions of the PS, SAS, SCDS, and PACS exist to meet the physical separation requirements of IEEE Std 603-1998, Clause 5.6.1. In addition, based on commitments to conform to RG 1.75, which provides guidance for meeting Class 1E physical separation requirements, the staff finds that redundant portions of the SICS, ICIS, EIS, BCMS, RMS, HMS, and RPMS, will meet the physical separation requirements of IEEE Std 603-1998, Clause 5.6.1. The staff finds the ITAAC provided to verify that physical separation exists between the four divisions of the PS, SAS, PACS, SCDS, and RPMS are adequate based on the acceptance criterion that the four divisions of these systems are located in separate Safeguard Buildings.

With regard to the Class 1E electrical divisions that power the controls and indications of the SICS, the staff finds that the ITAAC provided for physical separation is sufficient, based on the acceptance criterion that these Class 1E electrical divisions as listed in FSAR Tier 1, Table 2.4.2-1, are located in separate Safeguard Buildings

Based on the above findings, the staff concludes that the physical separation requirements of IEEE Std 603-1998 have been met.

#### 7.1.4.10.1.2 Electrical Isolation Between Redundant Portions of Safety Systems

FSAR Tier 2, Section 7.1.1.6.4, states that electrical isolation is required for hardwired and data connections, and is provided through the use of qualified isolation devices, and fiber optic cable. FSAR Tier 2, Section 7.1.2.5.9, "BTP 7-11 – Guidance on Application and Qualification of Isolation Devices," states that applicable I&C systems listed in FSAR Tier 2, Table 7.1-2, will be designed to meet the guidance of SRP BTP 7-11. FSAR Tier 2, Table 7.1-2, Interim Revision 3 mark-ups submitted as part of a June 22, 2011 response to RAI 442, Question 07.01-26, depicts the I&C systems that will be designed to meet the guidance of SRP BTP 7-11, which include the SICS, SCDS, PS, SAS, PACS, CRDCS, ICIS, EIS, BCMS, RMS, HMS, RPVLMS, and RPMS.

Based on the information provided in FSAR Tier 2, Section 7.1, Interim Revision 3 mark-ups, the staff finds the information provided is adequate to demonstrate that electrical isolation exists

between redundant portions of safety divisions to meet the electrical isolation requirements of IEEE Std 603-1998, Clause 5.6.1. Specifically, the staff finds the commitments to apply the guidance of SRP BTP 7-11 and to use qualified electrical isolation devices and fiber-optic cable for hardwired and data connections between redundant portions of safety systems are adequate to prevent electrical faults originating in one division from affecting redundant divisions.

The following ITAAC are provided in FSAR Tier 1, Interim Revision 3 mark-ups to verify that adequate electrical isolation exists between redundant portions of safety systems:

- Item 4.16 of FSAR Tier 1, Table 2.4.1-7, "Protection System ITAAC," verifies electrical isolation is provided on connection between the four PS divisions. The acceptance criterion to verify this commitment states, in part, that the Class 1E isolation devices used between the four PS divisions will prevent the propagation of credible electrical faults and that Class 1E electrical isolation devices exist on connections between the four PS divisions.
- Item 4.2 of FSAR Tier 1, Table 2.4.2-2, "Safety Information and Control System ITAAC," verifies electrical isolation exists between the Class 1E electrical divisions that power the control and indications of the SICS. The acceptance criterion that verifies this commitment is that the Class 1E electrical divisions that power the controls and indications of the SICS as listed in FSAR Tier 1, Table 2.4.2-1, are electrically isolated from each another.
- Item 4.6 of FSAR Tier 1, Table 2.4.4-6, "Safety Automation System ITAAC," verifies electrical isolation is provided on connections between the four SAS divisions. The acceptance criterion to verify this commitment states, in part, that the Class 1E isolation devices used between the four SAS divisions will prevent the propagation of credible electrical faults and that Class 1E electrical isolation devices exist on connections between the four SAS divisions.

The staff finds that the ITAAC provided to verify that electrical isolation exists between the four divisions of the PS and SAS are adequate. Specifically, the staff finds that the acceptance criterion that states that test reports will demonstrate that the Class 1E electrical isolation device used between the four PS and SAS divisions will prevent the propagation of electrical faults, is acceptable.

#### *7.1.4.10.2 Communication and Functional Independence*

The evaluation of communication and functional independence requirements to meet the requirements of GDC 21, GDC22 , GDC 24 and IEEE Std 603-1998, Clause 5.6.1, is provided in Section 7.9.4.6 of this report.

#### *7.1.4.10.3 Independence between Safety Systems and Effects of Design Basis Event*

IEEE Std 603-1998, Clause 5.6.2, states that safety system equipment required to mitigate the consequences of a specific DBE must be independent of, and physically separated from, the effects of the DBE to the degree necessary to retain the capability to meet the requirements of this standard. This clause specifies that equipment qualification in accordance with IEEE Std 603-1998, Clause 5.4, is one method that can be used to meet this requirement. In addition, 10 CFR Part 50, Appendix A, GDC 22, requires the PS to be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and

postulated accident conditions on redundant channels do not result in loss of the protection function.

To meet the requirements of IEEE Std 603-1998, Clause 5.6.2, safety systems shall meet the equipment qualification requirements of IEEE Std 603-1998, Clause 5.4, and, accordingly, provide sufficient diversity to prevent the loss of the safety functions. FSAR Tier 2, Section 7.1.2.6.15, states that equipment used in safety systems will be qualified using appropriate methods under the program described in FSAR Tier 2, Section 3.11, "Environmental Qualification of Mechanical and Electrical Equipment." Integrated system testing is performed as part of the TXS development process described in FSAR Tier 2, Section 7.1.1.2, to verify that the performance requirements of the safety functions have been met.

Evaluation for independence between safety systems and DBEs to meet the requirements of IEEE Std 603-1998, Clause 5.6.2, and GDC 22 is discussed as part of the evaluation for IEEE Std 603-1998, Clause 5.4, in Section 7.1.4.8 of this report. Based on the acceptable demonstration of equipment qualification in Section 7.1.4.8 of this report, the staff finds that the U.S. EPR design meets the requirements of IEEE Std 603-1998, Clause 5.6.2 and GDC 22.

#### *7.1.4.10.4 Independence between Safety and Non-Safety Systems*

IEEE Std 603-1998, Clause 5.6.3, requires safety system design to be such that credible failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of this standard. This clause consists of the following subclauses:

- Interconnected Equipment
- Equipment in Proximity
- Effects of a Single Random Failure

The evaluation of the U.S. EPR safety I&C system design for conformance to the requirements of IEEE Std 603-1998, Clause 5.6.3, is completed as part of the evaluation of each of the above subclauses. In addition, 10 CFR Part 50, Appendix A, GDC 24, requires the PS to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single PS component or channel which is common to the control system and PS leaves intact a system satisfying all reliability, redundancy, and independence requirements of the PS. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

The evaluation of communication and functional independence requirements to meet the requirements of IEEE Std 603-1998, Clause 5.6.3, is provided in Section 7.9.4.5 of this report.

##### *7.1.4.10.4.1 Interconnected Equipment*

For interconnected equipment, IEEE Std 603-1998, Subclause 5.6.3.1, requires:

- Equipment that is used for both safety and non-safety functions to be classified as part of the safety systems. Isolation devices used to affect a safety system boundary shall be classified as part of the safety system.
- No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and



following any DBE requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

FSAR Tier 2, Section 7.1.1.6.4, states that electrical isolation is provided for both hardwired and data communications between safety-related and non-safety-related I&C. For hardwired signals, qualified isolation devices are used with the safety-related I&C systems for signals to and from the non-safety-related I&C. Fiber optic cable is used for data connections between safety-related and non-safety-related I&C systems. This includes the use of fiber optic cables for the data connection between the PAS and the PACS. FSAR Tier 2, Section 7.1.2.5.9 states that applicable I&C systems listed in FSAR Tier 2, Table 7.1-2, Interim Revision 3 mark-ups, will be designed to meet the guidance of SRP BTP 7-11. FSAR Tier 2, Section 7.1.2.4.5 states that applicable I&C systems listed in FSAR Tier 2, Table 7.1-2 will be designed to meet the guidance in RG 1.75, which endorses IEEE Std 384-1992 with modifications. The I&C systems in FSAR Tier 2, Table 7.1-2, Interim Revision 3 mark-ups, that will be designed to meet the guidance of SRP BTP 7-11 and RG 1.75 include the SICS, SCDS, PS, SAS, PACS, CRDCS, ICIS, EIS, BCMS, RMS, HMS, RPLMS, and RPMS.

In addition, FSAR Tier 2, Section 7.1.1.6.4 states that data connections exist between the PAS and PACS. However, this connection is only between the PAS and non-safety-related portion PACS communication module. Connections between the communication module and safety-related priority module are hardwired. The communication module is qualified as an associated circuit. The PACS module will conform to the guidance of RG 1.75, which provides criteria for qualifying associated circuits.

The staff finds the information provided in FSAR Tier 2, Section 7.1, Interim Revision 3 mark-ups, regarding electrical isolation between safety and non-safety systems meets the requirements IEEE Std 603-1998, Clause 5.6.3, and GDC 24. Specifically, as specified in SRP BTP 7-11, fiber optical cables provide acceptable electrical isolation to prevent propagation of credible faults. As such, the staff finds the applicant's commitment to use isolation devices that are qualified in accordance with RG 1.75 for hardwired connections and use of fiber-optic cables for data connections acceptable in providing electrical isolation between safety and non-safety interfaces. In addition, the staff finds the qualification of the PACS communication module as an associated circuit in accordance with the guidance of RG 1.75 acceptable in ensuring that the failures in the communications module will not cause a failure of the PACS priority module.

#### 7.1.4.10.4.2 Equipment in Proximity

For equipment in proximity of safety systems, IEEE Std 603-1998, Subclause 5.6.3.2 requires:

- Equipment in other systems that is in physical proximity to safety equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1992.
- Physical barriers used to effect a safety system boundary shall meet the requirements of Clauses 5.3, 5.4 and 5.5 for the applicable conditions specified in Clause 4, items g) and h) of the design basis..

FSAR Tier 2, Section 7.1.1.6.4, states that safety-related I&C systems are physically separated from non-safety-related I&C systems. This section is supplemented by FSAR Tier 2, Section 7.1.2.4.5 which states that applicable I&C systems listed in FSAR Tier 2, Table 7.1-2, will be designed to meet RG 1.75.

Based on the applicant's commitment to provide physical separation between safety-related I&C systems and non-safety-related I&C systems in accordance with RG 1.75, the staff finds the applicant has adequately addressed the physical separation requirements of IEEE Std 603-1998, Clause 5.6.3.

The following ITAAC in FSAR Tier 1, Revision 3 mark-ups, was provided to verify adequate physical separation exists between Class 1E and non-Class 1E equipment:

- FSAR Tier 1, Table 2.4.1-7, "Protection System ITAAC," Item 2.3 verifies that physical separation exists between Class 1E PS equipment and non-Class 1E equipment.
- FSAR Tier 1, Table 2.4.2-2, "Safety Information and Control System ITAAC," Item 2.4 verifies that physical separation exists between safety-related part of the SICS and non-Class 1E equipment.
- FSAR Tier 1, Table 2.4.4-6, "Safety Automation System ITAAC," Item 2.3 verifies that physical separation exists between Class 1E SAS equipment and non-Class 1E equipment.
- FSAR Tier 1, Table 2.4.25-4, "Signal Conditioning and Distribution System ITAAC," Item 2.3 verifies that physical separation exists between Class 1E SCDS equipment and non-Class 1E equipment.
- FSAR Tier 1, Table 2.4.26-4, "Rod Position Measurement System ITAAC," Item 2.3 verifies that physical separation exists between Class 1E RPMS equipment and non-Class 1E equipment.

The acceptance criteria for these ITAAC include:

- A report exists and defines the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E safety equipment and non-Class 1E equipment.
- The required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E RPMS equipment and non-Class 1E equipment. Reconciliation is performed of any deviations to the design.

The staff finds the ITAAC provided to verify adequate physical separation exists between the Class 1E equipment of the PS, SICS, SAS, SCDS, and RPMS and non-Class 1E equipment are adequate by:

- Defining the structures, separation distance, barriers, or any combination thereof to achieve adequate separation between the Class 1E equipment and non-class 1E equipment
- Verifying that the as-built systems meet the defined required separation distance and barriers

#### 7.1.4.10.4.3 Effects of a Single Random Failure

For effects of a single random failure, IEEE Std 603-1998, Subclause 5.6.3.3, stipulates that where a single random failure in a non-safety system can result in a DBE, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure.

FSAR Tier 2, Section 7.1.1.6.4, states that safety-related I&C systems are implemented in four independent divisions. The safety-related I&C systems retain their ability to perform their function given a single failure of a common element to both the safety-related and non-safety-related systems concurrent with another single failure. The control systems implement signal selection algorithms and redundancy to minimize the possibility of a single failure that results in a DBE that also reduces the redundancy of the safety-related systems. The safety-related systems implement error detection algorithms to detect and accommodate failures.

As required by IEEE Std 603-1998, Clause 5.6.3.3 safety systems must retain the ability to perform safety functions in the presence of DBEs and single random failures of non-safety systems. Sections 7.1.4.5 and 7.9.4.6 of this report document the staff findings that the I&C safety systems will function independent of credible failures in interconnected equipment. Based on the information presented in FSAR Tier 2, Section 7.1.1.6.4, the staff did not identify any single random failure common to a non-safety system and a portion of the safety system that can result in a DBE and also prevent proper action of the remaining redundant portions of safety I&C equipment. As such, the staff finds the I&C systems design satisfies IEEE Std 603-1998, Clause 5.6.3.3.

#### 7.1.4.11 *Capability for Test and Calibration*

##### 7.1.4.11.1 *PS Test and Calibration*

The staff's review included the determination of whether IEEE Std 603-1998, Clause 5.7, has been adequately addressed for the U.S. EPR safety systems. IEEE Std 603-1998, Clause 5.7 requires capability for testing and calibration of safety system equipment while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. The capability should be provided to permit testing during power operation. GDC 21 requires, in part, that the PS shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred. RG 1.118, "Periodic Testing of Electric Power and Protection Systems," which endorses IEEE Std 338-1987, and RG 1.22, "Periodic Testing of Protection System Actuation Functions (Safety Guide 22)," provide guidance on periodic testing of the safety-related systems. The periodic testing should replicate, to the extent possible, the overall performance required of the safety systems. SRP Appendix 7.1-C, SRP Appendix 7.1-D, and SRP BTP 7-17 provide additional guidance on the capability for test and calibration for digital computer-based safety-related systems, which includes test provisions to address the increased potential for subtle digital system failures, and capabilities of the software to perform self test.

The staff reviewed the FSAR to verify that IEEE Std 603-1998, Clause 6.5, has been appropriately addressed. IEEE Std 603-1998, Clause 6.5 requires that means be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. The staff used SRP Appendix 7.1-C as guidance for reviewing compliance with IEEE Std 603-1998, Clause 6.5. Compliance with this requirement is documented in FSAR Tier 2, Section 7.1.2.6.32, "Capability for Testing and Calibration (Clause 6.5)." The applicant describes methods for compliance including perturbing the monitored variable, providing a substitute input to the sensor, and cross checking channels that have known relationships. These methods of sensor testing are described in FSAR Tier 2, Chapter 16. Computer-driven self-testing for sensor and acquisition circuits is also documented in FSAR Tier 2, Section 7.1, and Technical Report ANP 10315P "U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring" revision 1. Compliance with IEEE Std 603-1998, Clause 6.5 will be achieved upon a satisfactory evaluation for IEEE Std 603-1998, Clause 5.7.

FSAR Tier 2, Section 7.1.2.6.18, "Capability for Testing and Calibration (Clause 5.7)," states that the safety-related systems meet the requirements of IEEE Std 603-1998, Clause 5.7. The main safety-related systems include the PS, SAS, PACS, SCDS, SICS, and their integrated data communication system. FSAR Tier 2, Sections 7.1.2.2, 7.1.2.4, and 7.1.2.5, states that the design complies to GDC 22 and conforms to RG 1.22, RG 1.118, and SRP BTP 7-17, for all safety-related systems.

FSAR Tier 2, Sections 7.2.2.3.5, "Compliance to Requirements on System Testing and Inoperable Surveillance Requirements (Clause 5.7 of IEEE Std 603-1998)," and 7.3.2.3.6, "Compliance to System Testing and Inoperable Surveillance Requirements (Clause 5.7 of IEEE Std 603-1998)," address compliance to the requirement of IEEE Std 603-1998, Clause 5.7 for the RT and ESF functions, respectively. The applicant states that the design of the PS which includes RTS, ESFAS, and their interlock systems allows for testing of the RT and ESFAS functions while retaining the capability to perform the RT and ESFAS functions. The applicant also states that the PS design will retain its automatic actuation capability while under testing and that this capability is maintained during computer self-testing. Surveillance of the PS consists of overlapping tests to verify performance of the complete RT and ESFAS functions from sensor to field actuation devices. The functional units of the PS design are continuously monitored through self-testing during power operation. Sensors and acquisition circuits for the PS are periodically tested. In the PS design, the input channel to be tested is placed in a lockout condition, and the downstream voting logic is automatically modified to disregard the input being tested. The RT and ESFAS functions are still performed using the redundant input channels during the test.

For the RT system, the connections between the PS output circuits, the RT devices, and the RT devices can be tested during power operation. One division of the PS and one redundancy of the RT devices are tested at a time to avoid spurious RT. If reactor trip orders are generated during the test, the RT is performed normally. For the ESFAS, the PS design allows for testing of automatic ESF actuation functions while retaining the capability to perform the functions in response to an event requiring protective action. The connections between the PS output circuits and the PACS modules can be tested during power operation. One function of one division of the PS is tested at a time, and the outputs of the PACS modules are disabled so that the actuators are not affected by the test. If an ESF actuation order is generated during the time that a PACS module is in test mode, the outputs of the PACS module remain disabled until the PACS priority module exits test mode. The ESF actuation functions are still performed by redundant divisions.

In FSAR Tier 2, Section 7.4.2.2.4, "Testing," the applicant indicates that self and periodic testing for systems required for safe shutdown is implemented to detect failures that could prevent the execution of the safety-related functions. The U.S. EPR design includes measures to detect and identify failures during reactor operation in order to avoid long periods of operation with degraded safety-related I&C systems, structures, and components which might lead to a loss of function due to an accumulation of failures.

Topical Report EMF-2110, Section 2.7.1.1, describes the self-test features of the TXS platform. This includes self testing related to equipment subracks, function processors, input/output (I/O) modules, and communication means. The self-test features verify the functionality of the components that process the ESFAS functions, but do not interact with the ESFAS processing. The self-test features are performed at the end of the processing cycle, only after the safety tasks (i.e., processing of ESFAS logic) have been completed. The self-test features are executed with a lower priority than the ESFAS logic and the two are not performed at the same time. The staff discussion of the review of this associated ITAAC is provided in Section 14.3.5 of this report.

The U.S. EPR design certification application commits to RG 1.22, RG 1.118, and SRP BTP 7-17 for all safety-related systems. FSAR Tier 2, Section 7.1.1.4.2, includes a summary of data communication implemented within the SAS. Additional staff discussion is provided in Section 7.9.4.5 of this report.

In the FSAR, the applicant states compliance with Clause 5.7 in two specific ways:

- In terms of the inherent and engineered self test features to replace certain types of manual maintenance activities. The applicant takes credit for this application of self-test features in order to meet Clause 5.7.
- The self-test features themselves are part of the safety-related software and as such, must have their design function tested in a manner which, as closely as practicable, duplicates this design function.

Initially, the staff identified the following concerns with the applicant's stated compliance to Clause 5.7:

- There is no mention of SAS compliance, which is significant considering SAS has been designated by the applicant as a safety-related system and it performs safety-related closed loop controls in support of ESF actuations, as well as performing safety-related interlock functions.
- There are no design details in the FSAR concerning how the self-testing features are implemented and self-testing features coverage for either the PS or for SAS.
- The FSAR discussion of the compliance to Clause 5.7 did not provide information on how the automatic self-testing features are integrated into the overall surveillance and maintenance philosophy in the U.S. EPR design or how the automatic self-testing features add to the design's compliance to the requirements of Clause 5.7.
- There is no ITAAC verifying self-test functionality for the U.S. EPR design.

Given this summary of concerns, in RAI 59, Question 07.03-21, the staff requested that the applicant address the above issues. In a May 20, 2011, response to RAI 59,

Question 07.03-21, the applicant provided Technical Report ANP-10315, "U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report," Revision 0. The intent of this technical report was to provide the overall surveillance and self-testing philosophy as applied to the U.S. EPR PS. Technical Report ANP-10315, Figure 2-1 shows the overall surveillance program, in addition to demonstrating the physical scope of self-testing, in conjunction with manual testing features in the U.S. EPR design.

In Technical Report ANP-10315P, Revision 1, Section 2.1, the applicant states that self-test features are intended to replace the traditional channel checks and functional tests. The scope of the staff's review in this section includes analysis as to whether failures captured by traditional forms of maintenance and surveillance testing are enveloped by the self-testing features. The scope of the staff's review in this section does not approve the elimination and/or extension of Technical Specification surveillances outlined in Technical Report ANP-10315P, Revision 1. Refer to Chapter 16 of this report for more information on this aspect of the staff's review.

#### 7.1.4.11.1.1 Conformance with BTP 7-17

SRP BTP 7-17 states, in part, that self-diagnostic features should be verified periodically. The applicant addresses conformance to the guidance of SRP BTP 7-17 in Technical Report ANP-10315. In Technical Report ANP-10315, Section 3.6, the applicant states the following in regards to addressing periodic verification of self-test functions:

Self-test functionality is not directly tested via periodic functional testing. To do so would require injection of faults into the safety system; which is neither prudent nor necessary. It is not prudent because it risks permanent damage to the safety system that may prevent correct functioning in the future and because it would be difficult to determine that the injected fault had been completely "removed" from the system following testing.

The staff's concern centers on the capability for the self-test features to continue performing their functions for the life of the system. The applicant states that it would be difficult to determine if an injected fault was completely removed following testing. The staff considers the self-test features an essential aspect of the TXS platform considering that credit is being taken for surveillance testing by using the self-test features.

The applicant also states that direct testing of self-testing features is not necessary due to their functions being verified by the following means.

#### Method of Verification 1:

Indirect periodic testing: The function processors and communication paths are exercised as part of other surveillance testing as described in Sections 2.2.1 through 2.2.5. This verifies that faults resulting in the inability of the equipment to perform its safety function would be detected. Such faults should be detected by self-tests and, if such a fault is detected during other surveillance testing, then incorrect operation of the self-test features are also detected.

According to the applicant, the self-testing features exist, individually, on each TXS function processor. The staff disagrees that exercising the function processors and communication paths during the performance of other surveillance testing, verifies the full design functionality of the inherent and engineered self monitoring that exists on each function processor. The

applicant does not provide details on what it means by “exercising” function processors and how this exercising provides direct information or insight into self-testing functionality. Secondly, the applicant states that such faults during this exercising “should” be detected by self-tests. The staff considers this language ambiguous. In Technical Report ANP-10315, the applicant provides a definitive listing of the all the various types of failures that automatic self-tests will detect. Because the applicant has provided a definitive list of failures that the automatic self-test features can detect, the staff finds the ambiguity introduced by this method of verification unacceptable. Third, the self-test features perform numerous tasks, such as the prevention of control function initiation while maintenance or surveillances are being performed with the Service Unit (SU). The applicant has not provided enough information in this method for the staff to understand how this design aspect, as well as the other self-test functions stated in Technical Report ANP-10315, revision 1, is verified.

#### Method of Verification 2:

Self-test qualification and configuration control: The TXS system software, including the software used in the self-test process, is developed and tested using a quality program as described in Reference 10. This verifies that the self-test features function properly. TXS system software contains an identification file providing a CRC [cyclic redundancy check] checksum for all files which are delivered within a package (e.g., executable programs, dynamic-link libraries, object modules, pre-links, header files). The CRC checksum of the complete TXS system software installation forms a unique identification of the version. When the TXS system software is loaded onto the TXS processing unit, the CRC checksum of the loaded TXS system software on the TXS processing unit is manually verified to match the CRC checksum of the originally developed and tested TXS system software. This verifies that the system software containing self-test features is identical to that which was tested and verified to operate correctly.

Verifying the operation of self-test features and verifying the design function of the self-test features are two distinct actions. The staff agrees that development and maintenance of the self-test features as safety-related software provides assurance that the self-test features have sufficient quality to perform their functions. Maintenance of the self-test features would be captured under the quality design change process for safety software. However, the applicant has not addressed the full range of capabilities of the self-test features to perform all of their credited actions. Specifically, if there are hardware aspects of the TXS self-test features that could degrade over time, the self-test feature may be degraded. For example, the TXS platform utilizes a hardware watchdog timer. Hardware devices, such as timers, relays, etc., can degrade over time and fail to function properly. At a minimum, periodic testing should be performed on the hardware aspects of the self-testing features to verify their operation.

### Method of Verification 3:

Continuous monitoring of the self-test: Two mechanisms are used to continuously monitor correct operation of the self-test: the hardware watchdog timer and the runtime environment. The hardware watchdog timer (described in Section 2.2.6.2) will trip if a failure in the self-test features causes a stop of the function processors cyclic operation. The runtime environment initiates an alarm if the complete set of self-test routines is not completed within one hour.

Technical Report ANP-10315, Section 2.2.6.2, describes the operation of the hardware watchdog timer, which is considered part of the inherent TXS monitoring features. The applicant states that each TXS function processor is equipped with a hardware-based watchdog timer. The staff considers the hardware watchdog timer a part of the self-test features. The hardware watchdog timer must be re-triggered by the run-time environment (RTE) before its expiration, or an error is assumed and a hardwired signal is used to indicate processor failure, switch off the I/O module power supply to place the affected processor in a defined failure state, and activate the exception handler. These actions are independent of the inherent self-monitoring software. The second mechanism mentioned is the RTE. This mechanism is based entirely on inherent functions of the TXS. This mechanism does not verify the full design functionality of the inherent and engineered monitoring features but does ensure that the self test routines are performed within a given period of time. Both mechanisms are functional aspects of the inherent monitoring features.

### Method of Verification 4:

Periodic extended self-test: The periodic initiation of the extended self-test includes checks of the memory containing the cyclic self-test software, and a CRC check to verify that the system software containing the self-test routines is identical to the routines initially loaded onto the function processor.

The extended self-test is initiated when a function processor is reset. Similar to Method of Verification 2, the extended self-test verifies the integrity of the self-test software that exists on the function processor. The staff's key concern regarding this method is the timeframe for which it will be performed. In Technical Report ANP-10315P, the applicant did not state that periodically restarting function processors is a part of normal surveillances or other type of maintenance. Because resetting of a function processor would likely be a random event, based on a failure of some type or maintenance, this method of verification cannot be counted on as a means to ensure self-test functionality on a periodic basis.

For the indirect methods provided, the applicant did not state in Technical Report ANP-10315, Revision 1, that the observance of these methods would be entered into a surveillance or maintenance program or some other type of program with approved procedures that would provide any controls. Also, if the applicant does not intend to directly test the self-testing feature of the U.S. EPR design, the staff questions how certain portions of the PS design will be verified during plant operation. For example, if the hardware watchdog timer fails to initiate a signal of processor failure, the resulting processor outputs, and its associated safety equipment, could be left in an undefined state versus a defined failure state. Therefore, in RAI 505, Question 07.01-39, the staff requested that the applicant address the above issues associated with periodic self-testing. **RAI 505, Question 07.01-39 is being tracked as an open item.**



#### 7.1.4.11.1.2 Conformance with IEEE Std 7-4.3.2-2003

RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Std 7-4.3.2-2003. IEEE Std 7-4.3.2-2003, Clause 5.5.3 states, in part, that when self-diagnostics are applied, the following self-diagnostic features shall be incorporated into the system design:

- Self-diagnostics during computer system startup
- Periodic self-diagnostics while the computer system is operating
- Self-diagnostic test failure reporting

Technical Report ANP-10315, Section 2.2.6.1 states that an extended self-test is performed during every startup of each function processor. It is automatically initiated during the resetting of a function processor. The extended self-test includes certain testing that cannot be performed during normal operations of a function processor due to the potential to interfere with the processing of the application software that resides on the function processor. If an error is detected during the extended self-test, the function processor's cyclic processing is stopped, preventing operation in the runtime environment. Technical Report ANP 10315, Table 2-1 documents which components undergo startup testing.

The staff finds the design of the self-test features adequately conforms to the guidance provided by IEEE Std 7-4.3.2-2003. As stated above, TXS function processors perform extended testing each startup as part of the normal startup routine. Failures detected during startup result in the processor's cyclic processing being halted with no communication from the affected function processor being possible. The staff considers this an adequate level self-testing during startup.

Table 7.1-1 below identifies the self-testing features of the U.S. EPR design that are continuous and performed while the plant is online. Technical Report ANP-10315, Table 2-5 shows the overall coverage of the self-testing features. Continuous monitoring is performed from the start-up of a function processor and continues throughout its cyclic processing state as well as with other communication modules and network equipment. The staff finds that the design adequately addresses the periodic testing of computer equipment while it is in operation.

**Table 7.1-1 Self-Testing Features in U.S. EPR Design**

Self-test Type	Monitoring Features	Actions Initiated
Inherent Monitoring Features – built into the TXS platform and are integrated onto each function processor. Part of the RTE.	<ul style="list-style-type: none"> <li>• Hardware Watchdog Timer</li> <li>• Communication Monitoring (e.g., CRC checks)</li> <li>• Startup testing</li> <li>• Continuous self-tests</li> <li>• Error code monitoring of RTE equipment such as function processors, communication and network equipment</li> </ul>	<ul style="list-style-type: none"> <li>• Initiation of the Exception Handler</li> <li>• Extended self-test during startup routine of function processor</li> <li>• Error messages transferred to SU</li> <li>• Prevents faulted function processor from starting cyclic processing</li> </ul>
Engineered Self-Monitoring	<ul style="list-style-type: none"> <li>• Monitoring RTE message flags to</li> </ul>	<ul style="list-style-type: none"> <li>• Initiation of alarms or</li> </ul>

Self-test Type	Monitoring Features	Actions Initiated
Features – These features operate in the application layer and are designed on a project-specific basis.	<p>use in alarm processing</p> <ul style="list-style-type: none"> <li>Monitoring status of signal inputs</li> <li>Channel Check – Analog input measurements from each safety division are sent to the divisional MSIs, then on to the gateways. At the gateway, signals from redundant divisions are compared for consistency. Inconsistent measurements trigger a MCR indication.</li> <li>Monitoring of ranges of signal input values, such as live-zero monitoring, which means if a signal, such as a 4-20mA signal falls below 3.5mA, the self-tests would consider this a faulty signal.</li> </ul>	<p>other indication in MCR</p> <ul style="list-style-type: none"> <li>Mark affected signals as faulty and exclude from further processing by other function processors</li> <li>Initiate specific actions such as using a replacement value or triggering/blocking an I&amp;C function, especially in the case of multiple faults</li> </ul>

In terms of a failure of the self-testing features, Technical Report ANP-10315, Section 2.2.6.1 states:

If the continuous self-test is not complete after one hour, the runtime environment issues an error message to the SU. This error message is also transferred to the application software for inclusion in engineered alarms to the operator.

Technical Report ANP-10315, Section 2.2.6.2 describes the watchdog timer, which is hardware-based and exists on each TXS function processor. The watchdog timer is required to be re-triggered by the runtime environment software on each function processor before the timer expires. Failure of the software to perform this action results in a hardwired signal being issued, indicating a processor failure and to switch off the I/O module's power supply. This results in the function processor failing in a predefined safe state. All these actions take place independently of software-based monitoring stated previously.

The staff finds the design of the watchdog timer for monitoring of the self-testing features acceptable. The staff finds the implementation of the software-based monitoring inadequate based on information provided in Technical Report ANP-10315, Section 2.2.6.6. The staff is unclear as to why failures detected by software-based test features are not significant enough to warrant an automatic interruption of the affected function processor. This would be consistent with how a failure sensed by the watchdog timer is handled. If a failure of self-test detected by software monitoring results in the same actions as a failure detected by the watchdog timer, the staff has not found this information documented. As Technical Report ANP-10315, Section 2.2.6.6 is currently written, a TXS function processor could continue running indefinitely without any continuous self-tests being performed, because no interruption of operations occurs. Therefore, in RAI 505, Question 07.01-40, the staff requested that the applicant address this issue. **RAI 505, Question 07.01-40 is being tracked as an open item.**

The staff noted that Technical Report ANP-10315 does not indicate what the TXS-based systems will do if the inherent monitoring or engineered monitoring features detects a faulty

component. The report does not provide a description of what automatic steps are taken by the system to identify the problem device, isolate, or disable outputs, and then state what happens to other devices that are part of downstream logic, or are sharing information with the problem device. In addition, FSAR uses numerous terms to identify how outputs are treated during various types of device malfunction. Terms such as “halted,” “disabled,” and “out of service” are cited in FSAR and Technical Report ANP-10315 when describing how outputs on a known malfunctioning device are automatically treated by the U.S. EPR design. Therefore, in RAI 505, Question 07.01-41, the staff requested that the applicant to address these issues. **RAI 505, Question 07.01-41 is being tracked as an open item.**

The SU is the device that technicians would use to perform maintenance and surveillance testing for the TXS platform. In Technical Report ANP-10315, Section 2.2.6.1, the applicant states, in part, the following:

Any errors detected by the extended self-test prevent the function processor from starting its cyclic processing. The function processor does not complete its startup, but instead enters an endless loop allowing for diagnosis using the maintenance laptop. The maintenance laptop connects to the card front serial interface and communicates only with this single processor while connected.

In this circumstance, when the function processor exhibits a failure, its cyclic processing is stopped, and presumably, is no longer functioning within the RTE of the TXS platform. The SU communicates to each function processor through the RTE; therefore, if a function processor’s cyclic processing is stopped, the SU cannot be used to perform any type of maintenance or surveillance testing on that device. Due to this design feature, a local connection to the faulted processor is required to be made using a separate computer. According to Topical Report EMF 2110, Revision 1, this local connection is a serial port located on the front plate of each function processor on an equipment rack. The applicant provides no further detail on this arrangement in Technical Report ANP-10315. As indicated in the quote above, this device is referred to as a maintenance laptop. According to Section 2.2.6.1 of Technical Report ANP-10315, the maintenance laptop performs three functions:

- Initial Software Loading: The initial software load is made using the TXS maintenance laptop. Bootstrap loading of any TXS processor is not possible via the SU, since that type of connection requires TXS system software, application software, and pre-defined communication links installed. The maintenance laptop is also used to configure the communication modules.
- Post-Initial Software Loading: When the initial software load is complete, the maintenance laptop must be used to install software on a new processor board (e.g., after maintenance replacement) or to install system software upgrades. The maintenance laptop can also be used to load application software revisions on processor boards (e.g., during an outage or if the service unit is not available).
- Diagnostic Information Retrieval: The maintenance laptop can be used to retrieve diagnostic failure information from the exception handler buffer to diagnose failures. However, this use is not a typical user maintenance activity but may be used during commissioning testing. The maintenance laptop cannot access other local software when in diagnostic monitor mode.

According to the applicant, the laptop is loaded with software such as the Linux operating system, SPACE tool, Oracle database, and TXS support for Linux. The staff has not been able to determine what isolation is available when utilizing the maintenance laptop. In terms of safety-qualification, in Technical Report ANP-10315P, Section 3.6, the applicant states that the SU and test machines do not perform any safety-related function and the digital computer equipment is appropriately qualified for its function. The staff understands that the maintenance laptop and other test machines referenced in Technical Report ANP-10315P are classified as non-safety-related. The implication of this design is that making a direct connection, with no level of data or electrical isolation to a non-safety-related diagnostic computer would pose concerns for sufficient independence. In the case of the SU, it connects to a PS division or SAS division by way of an MSI. The applicant did not address in Technical Report ANP-10315P how guidance from SRP BTP 7-17 or ISG-04 Staff Position 1, Points 10 and 11, are met with regards to this connection, or whether this type of connection scenario applies to all TXS safety systems. Therefore, in RAI 505, Question 07.01-34, the staff requested that the applicant address these issues. **RAI 505, Question 07.01-34 is being tracked as an open item.**

The applicant makes generic references to “test machines” throughout Technical Report ANP-10315P. In particular, ANP-10315P, Section 2.2.2 makes reference to a “portable test machine”. Technical Report ANP-10315P, Figure 2-2 illustrates the test machine which appears to be a laptop. The applicant did not provide sufficient information with regards to the use and connections of the test machine(s) for the staff’s evaluation. Therefore, in RAI 505, Question 07.01-34, the staff requested that the applicant address this issue. **RAI 505, Question 07.01-34 is being tracked as an open item.**

#### *7.1.4.11.2 SAS Test and Calibration*

FSAR Tier 2, Section 7.4.2.2.4, states that self and periodic testing for systems required for safe shutdown is implemented to detect failures that could prevent the execution of the safety-related functions. Technical Report ANP-10315, Revision 1 states that only Section 2.2.6 (Self Monitoring Features) is generically applicable to any system implemented with TXS microprocessor-based technology, which would include SAS. Technical Report ANP-10315P, Revision 1, addresses the overall surveillance testing program for the U.S. EPR I&C design. In Technical Report ANP-10315P, Revision 1, Section 1.2, the applicant addresses the overall surveillance testing program for the I&C design. In Technical Report ANP-10315P, Revision 1, Section 1.2, the applicant states that the surveillance testing portion of the report applies only to the PS. In RAI 505, Question 07.01-42, the staff requested that the applicant address surveillance testing on the other safety-related I&C systems, including SAS, which have Technical Specification surveillance requirements. **RAI 505, Question 07.01-42 is being tracked as an open item.**

#### *7.1.4.11.3 SICS Test and Calibration*

FSAR Tier 1, Section 2.4.2, does not provide any design information for self-test features in the SICS design. FSAR Tier 1, Table 2.4.2-2, does not contain any ITAAC that verifies the self-testing aspect of the SICS design. The scope of the self-testing features for PS and SAS may envelope the SICS; however, this is not clear to the staff based on the review of documentation available. In addition, FSAR Tier 2, Revision 3, Table 7.1-4, “DCS Interface Matrix,” shows that SICS manual controls to PS and SAS are hardwired and would not be subject to automatic self-testing. Therefore, self-testing coverage would be questionable. In RAI 505, Question 07.01-43, the staff requested that the applicant clarify the self-test features of SICS for both FSAR Tier 1 and FSAR Tier 2 design descriptions and address the need for any

ITAAC to verify the self-test features. **RAI 505, Question 07.01-43 is being tracked as an open item.**

#### *7.1.4.11.4 Test And Calibration For Other TXS Safety-Related Systems*

FSAR Tier 2, Section 7.1.2.6.18, states that the safety-related systems meet the requirements of IEEE Std 603-1998, Clause 5.7. Besides the systems stated in this section of the report, it is unclear to the staff what other safety-related systems credit self-testing features. FSAR Tier 2, Section 7.1.2.6.18, refers only to FSAR Tier 2, Sections 7.2 and 7.3, which are the RT and ESF systems, respectively. These sections do not necessarily contain design information reflective of the other safety-related TXS I&C systems. Technical Report ANP-10315 does not provide the staff a clear understanding of other safety-related I&C systems (besides PS and SAS) that implement credited self-test features. However, scope and design of the self-test features for the PS and SAS may provide coverage for the other safety-related I&C systems. Therefore, in RAI 505, Question 07.01-44, the staff requested that the applicant address this issue. **RAI 505, Question 07.01-44 is being tracked as an open item.**

#### *7.1.4.11.5 PACS Test and Calibration*

Technical Report ANP-10310P, Revision 1, states the infrastructure signals of the PACS are processed by self-monitoring features on the PLD. The PLD is the safety-related priority module and would fall under IEEE Std 603-1998 Clause 5.7. The applicant has taken credit for the overall U.S. EPR design's self-testing features to meet the requirements of IEEE Std 603-1998 Clause 5.7. Therefore, this includes any self-monitoring features associated with the PACS. However, Technical Report ANP-10315P does not address the self-monitoring features of the PACS. Also, FSAR Tier 1, Section 2.4.5, Interim Revision 3 mark-up, does not verify PACS self-testing functionality. Information on the PACS self-monitoring is not discussed in FSAR Tier 2. In addition, infrastructure signals provide a significant function in terms of ESF operations. GDC 23 requires, in part, that upon failure, the PS fail into a safe state or into a state demonstrated to be acceptable on some other defined basis upon a loss of electrical power or postulated adverse environments. The PLD, by means of self-testing features, is responsible for this action. In RAI 505, Question 07.01-45, the staff requested that the applicant address the issue of PACS self-testing. **RAI 505, Question 07.01-45 is being tracked as an open item.**

#### *7.1.4.12 Information Displays*

The staff reviewed U.S. EPR design certification application to verify that IEEE Std 603-1998, Clause 5.8, has been adequately addressed for the U.S. EPR safety systems. IEEE Std 603-1998, Clause 5.8.1, states, in part, that the display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE 497-1981, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. FSAR Tier 2, Section 7.1.2.6.19, states that safety-related systems meet the requirements of IEEE Std 603-1998, Clause 5.8 and the U.S EPR displays address the criteria in IEEE Std 497-2002. RG 1.97, Revision 4, endorses IEEE Std 497-2002 as meeting the intent of the former IEEE 497-1981. Furthermore, displays and control are provided by the SICS for those manual actions described in FSAR Tier 2, Chapter 15, "Transient and Accident Analyses." FSAR Tier 2, Section 7.1.2.6.19, states that safety-related systems provide to the PICS their

bypassed and inoperable status to allow the operator to identify the specific bypassed functions and determine the state of actuation logic.

SRP Appendix 7.1-C states that bypassed and inoperable status indication should conform to the guidance in RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." FSAR Tier 2, Section 7.1.2.1.4, "10 CFR 50.34(f)(2)(v) – Bypass and Inoperable Status Indication," states that the applicable I&C systems listed in FSAR Tier 2, Table 7.1-2, are designed to meet the requirements of 10 CFR 50.34(f)(2)(v). This is provided by compliance with IEEE Std 603-1998, Clauses 5.8.2 and 5.8.3. Specifically, the applicant states in FSAR Tier 2, Section 7.5.2.2.4, "Conformance to Regulatory Guide 1.47," that if a protective function of some part of a safety system has been bypassed or deliberately rendered inoperable, continued indication of the bypassed condition is provided in the MCR. In addition, the applicant states in FSAR Tier 2, Section 7.5.2.1.1, "10 CFR 50.34(f), 'Additional TMI Related Requirements'," if any PAM Type A, B, and C variable is bypassed or rendered inoperable, an indication is provided to the operator in the MCR. The PS and the SAS provide display signals to the PICS. Outputs to PICS from safety-related systems are supplied through qualified isolation devices. If the PS or SAS is operated in a bypassed mode or inoperable condition, an output is automatically provided to the PICS for indication of the bypass or inoperable condition in accordance with the guidance of RG 1.47 and IEEE Std 603-1998, Clause 5.8.3.

The applicant states that I&C systems listed in FSAR Tier 2, Table 7.1-2, meet IEEE Std 603-1998, Clauses 5.8.3(c) and 5.8.4. IEEE Std 603-1998, Clause 5.8.3(c), states that the capability shall exist in the control room to manually activate the display indication. In addition, IEEE Std 603-1998, Clause 5.8.4, states that information displays shall be located accessible to the operator, and that information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions. FSAR Tier 2, Section 7.1.2.1.4, also states that the applicable I&C systems listed in FSAR Tier 2, Table 7.1-2, are designed to meet the requirements of 10 CFR 50.34(f)(2)(v).

The staff reviewed the above commitments and finds that sufficient design information is provided to meet IEEE Std 603-1998, Clause 5.8. Specifically, the applicant commits to RG 1.47 and RG 1.97 regarding bypass or inoperable conditions and post-accident monitoring variables. The staff compared the safety functions in FSAR Tier 2, Chapter 15 to the available manual actions. The staff noted that the U.S. EPR credits operator action for a steam generator tube rupture. Safety-related, division-level manual controls are available to perform the necessary operator actions for a steam generator tube rupture. In addition, the staff review of human factors in Chapter 18 of this report addresses the adequacy of information presentation to operators. Based on the commitments provided, the staff finds the U.S. EPR design meets the requirements of IEEE Std 603-1998, Clause 5.8. GDC 13 requires, in part, that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Based on compliance to IEEE Std 603-1998, Clause 5.8 and the commitments provided in FSAR Tier 2, the staff finds that the U.S. EPR design meets GDC 13. Additional discussion on information displays important to safety is provided in Section 7.5.4 of this report.

#### 7.1.4.13 *Control of Access*

IEEE Std 603-1998, Clause 5.9 requires that the safety system design permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station, or by a

combination thereof. SRP Appendix 7.1-C provides acceptance criteria to address the clauses of IEEE Std 603-1991. These criteria also apply to IEEE Std 603-1998, SRP Appendix 7.1-C, Clause 5.9, states that administrative control is acceptable to assure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access. The review of access control should confirm that design features provide the means to control physical access to safety system equipment, including access to test points and means for changing setpoints. Typically, such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located. Review of digital computer-based systems should consider controls over electronic access to safety system software and data. Controls should address access via network connections, and via maintenance equipment.

The staff reviewed the U.S. EPR design certification application to verify that IEEE Std 603-1998, Clause 5.9 has been adequately addressed for the U.S. EPR data communication systems, including the SU access to the safety system, as documented in Section 7.9.4.3 of this report. This review is focused on the logical access control to safety systems.

The staff reviewed the U.S. EPR TXS-based I&C systems to verify conformance to the secure development and operational environment (SDOE) requirements. This review was completed as part of the safety evaluation for Topical Report ANP-10272, "Software Program Manual for TELEPERM XS™ Safety Systems," Revision 3.

FSAR Tier 2, Section 7.1.2.6.20, "Control of Access (Clause 5.9)," Interim Revision 3 mark-ups, states that the safety systems meet the requirements of IEEE Std 603-1998, Clause 5.9. This section states that access to the cabinets of the SICS, PS, SAS, SCDS, and PACS are provided via doors that are normally closed and locked. Door positions are monitored, allowing operators the ability to investigate unexpected opening of cabinet doors. Cabinets are also located in physically separate equipment rooms within the four Safeguard Buildings and can only be accessed by authorized personnel. FSAR Tier 2, Table 7.1-6, "Function Processor Operational States," Interim Revision 3 mark-ups, states that changeable parameters, including setpoints, may be modified when the safety function processor is in the parameterization mode. FSAR Tier 2, Section 7.1.1.6.4, Interim Revision 3 mark-ups, describes the access controls to prevent changing the safety processor operational modes. This includes access controls to the safety function processor CPU state switch, which enables the SU to change the operational mode of the CPU. In addition, a separate hardwired disconnect exists between the SU and the safety function processors during normal operation. The evaluation of the hardwired disconnect and CPU state switch is documented in Section 7.9.4.3 of this report. For maintenance bypass, FSAR Tier 2, Section 7.1.2.6.34, states that individual function computers of the PS, and SAS can be placed into testing and diagnostic modes via the SU. In the testing and diagnostic mode, the outputs of the function processor are disabled and therefore considered bypassed. The logical access controls on the SU, as well as the safety function processor CPU state and cabinet locks, prevent unauthorized bypasses of the safety systems. For operating bypasses, FSAR Tier 2, Section 7.1.2.6.33, "Operating Bypass (Clauses 6.6 and 7.4)," states that operating bypasses are implemented using permissive signals from the PS. FSAR Tier 2, Section 7.2.1.3, "Permissive Signal Functional Description," Interim Revision 3 mark-ups, states that the operator may activate manual permissives from the SICS. The SICS interface is located in the MCR and RSS, which have access controls to prevent unauthorized access.

Based on the provisions for cabinet locks, door position monitors, and alarms for the SICS, PS, SAS, SCDS, and PACS, the staff finds that the physical access controls for the SICS, PS, SAS, SCDS, and PACS are adequate to prevent unauthorized access and modification to the safety I&C systems. This includes providing access controls to the means for bypassing safety system functions and to prevent unauthorized modifications to setpoints. Therefore, the staff finds that the U.S. EPR safety I&C systems meet the requirements of IEEE Std 603-1998, Clause 5.9.

The following ITAAC in FSAR Tier 1, Interim Revision 3 mark-ups, were provided to verify adequate physical control of access exists for safety equipment:

- FSAR Tier 1, Table 2.4.1-7 Item 4.20 verifies that locking mechanisms are provided on the PS cabinet doors. Opened PS cabinet doors are indicated in the MCR.
- FSAR Tier 1, Table 2.4.4-5, Item 4.12 verifies that locking mechanisms are provided on the SAS cabinet doors. Opened SAS cabinet doors are indicated in the MCR.
- FSAR Tier 1, Table 2.4.5-3, Item 4.6 verifies that locking mechanisms are provided on the PACS cabinet doors. Opened PACS cabinet doors are indicated in the MCR.

The acceptance criteria for these ITAAC include:

- Locking mechanisms exist on the system's cabinet doors
- The locking mechanisms on the system's cabinet doors operate properly
- Opened cabinet doors are indicated in the MCR

The staff finds the ITAAC provided to verify the control of access features in the PS, SAS, and PACS are adequate based on the verification that locking mechanisms exist and operate correctly on the cabinet doors and that indications are provided in the MCR for opened cabinet doors. However, the staff finds that an ITAAC was not provided to verify physical access control features exist on the cabinets of the SICS, SCDS, and RPMS. Therefore, in RAI 506, Question 14.03.05-37, the staff requested that the applicant provide an ITAAC to verify that these features exist and operate for the SICS, SCDS, and RPMS cabinets to prevent unauthorized access to the systems. **RAI 506, Question 14.03.05-37 is being tracked as an open item.**

#### 7.1.4.14 *Repair*

The staff reviewed U.S. EPR design certification application to verify that IEEE Std 603-1998, Clause 5.10 has been adequately addressed for the EPR safety systems. IEEE Std 603-1998, Clause 5.10 requires that the safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Appendix 7.1-C, Section 5.10 states that digital safety systems may include self-diagnostic capabilities to aid in troubleshooting. However, the use of self-diagnostics should not replace the need for the capability for test and calibration systems. SRP BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions Review Responsibilities," describes characteristics that digital computer-based diagnostic systems should exhibit. For the digital computer-based systems, the surveillance testing with automatic self-testing should be provided to detect all detectable failures and assist the repair work.



FSAR Tier 2, Section 7.1.2.6.21, "Repair (Clause 5.10)," states that the safety systems meet the requirements of IEEE Std 603-1998, Clause 5.10, and that safety systems built upon the TXS platform contain self-diagnostic test features to detect both hardware and software faults and assist in diagnostic and repair activities as outlined in Topical Report EMF-2110. Additional details are provided in FSAR Tier 2, Section 7.3.2.3.6 for compliance to system testing and inoperable surveillance requirements.

The applicant indicates that the self-diagnostic features of the TXS platform are verified to function as designed by independent qualification, and that this is described in Topical Report EMF-2110, Sections 2.1.2 and 3.2. During plant operation, self-diagnostic functionality is performed during time intervals when no cyclic processing of the application software is active. It consists of a sequence of predefined monitoring tasks. If this sequence is not completed within a predefined amount of time, an error is generated. The TXS platform contains self-diagnostic test features to detect both hardware and software faults and to assist in diagnostic/repair activities as outlined in Technical Report ANP-10315. Technical Report ANP-10315 is applicable to both PS and SAS for design details concerning the self-test features only. Faults are alerted to the operator upon occurrence. FSAR Tier 1, Section 2.4 also provides details on the PS self-test features as well as providing FSAR Tier 1, Table 2.4.1-7, ITAAC Item 4.26, that gives the applicant's commitment to verify self-test functionality. Based upon the above information, the staff finds that compliance with IEEE Std 603-1998, Clause 5.10 is contingent upon the design meeting the requirements of IEEE Std 603-1998, Clause 5.7 for all safety systems that implement self-testing features that are credited. The evaluation of IEEE Std 603-1998, Clause 5.7 is discussed in Section 7.1.4.11 of this report.

#### 7.1.4.15 *Identification*

The staff reviewed the U.S. EPR design certification application to verify that IEEE Std 603-1998, Clause 5.11 has been adequately addressed for the U.S. EPR safety systems. IEEE Std 603-1998, Clause 5.11 requires that (1) safety system equipment be distinctly identified in accordance with the requirements of IEEE Std 384-1992, (2) components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification, (3) identification of safety system equipment be distinguishable from other purposes, (4) identification of safety system equipment does not require frequent use of reference material, and (5) the associated documentation be distinctly identified.

FSAR Tier 2, Section 7.1.2.6.22, "Identification (Clause 5.11)," states that safety-related systems meet the requirements of IEEE Std 603-1998, Clause 5.11 and the additional guidance of IEEE Std 7-4.3.2-2003. The applicant states that redundant divisions of each safety-related system are distinctively marked, versions of hardware are marked accordingly, and configuration management is used for maintaining identification of safety-related software. In RAI 75, Question 07.02-15 and RAI 75, Question 07.03-17, the staff requested that the applicant provide the location of the ITAAC that verifies appropriate identification of safety-related I&C components. In a June 12, 2009, response to RAI 75 Question 07.03-15, the applicant stated that FSAR Tier 1, Section 2.4.1, ITAAC Item 4.19, provides a verification of these design requirements in that the equipment for each PS division is distinctly identified and distinguishable from other divisional equipment by identifying markings placed on the equipment which do not require frequent use of reference material.

In summary, the staff finds that the U.S. EPR design adequately addresses IEEE Std 603-1998, Clause 5.11, and that there is adequate ITAAC to verify the design commitment to distinctly identify and mark safety-related equipment.

#### 7.1.4.16 *Auxiliary Features*

The staff reviewed the U.S. EPR design certification application to verify that IEEE Std 603-1998, Clause 5.12 has been adequately addressed for the U.S. EPR safety systems. IEEE Std 603-1998, Clause 5.12 states that (1) auxiliary supporting features shall meet all requirements of this standard, and (2) other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, and are part of the safety system by association, shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level.

In FSAR Tier 2, Section 7.1.2.6.23, the applicant states that the safety systems meet the requirements of IEEE Std 603-1998, Clause 5.12. The safety-related auxiliary supporting systems include EUPS, Class 1E power supply system (EPSS), and safety-related heating, ventilation, and air conditioning (HVAC) systems throughout the plant and are described in Chapter 8 and Chapter 9 of the FSAR. The applicant also indicates that other auxiliary features that are not required to be operable for the safety systems to perform their functions are designed to meet criteria that do not degrade the safety functionality of the safety systems below an acceptable level. However, the applicant does not specify what the other auxiliary features are in the design certification application. Based upon review guidance from SRP Appendix 7.1-C, SRP BTP 7-9, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," and other applicable guidance, the staff finds that to complete this review the applicant would need to provide additional information. In RAI 75, Question 07.02-16, the staff requested that the applicant describe other auxiliary features that are not required to be operable for the safety systems. In a January 14, 2009 response to RAI 75, Question 07.02-16, the applicant stated that the auxiliary features that are not required to be operable for the safety I&C systems are those features provided through the SU. These features include authorized software modifications, functional tests and periodic tests, monitoring of correct processing, and fault detection and failure diagnosis. The SU requests access to the safety-related processors through the MSIs. Additional staff discussion related to the SU is also provided in Section 7.9.4 of this report. Based on the commitment for necessary auxiliary features and their design, the staff finds the U.S. EPR design meets IEEE Std 603-1998, Clause 5.12.

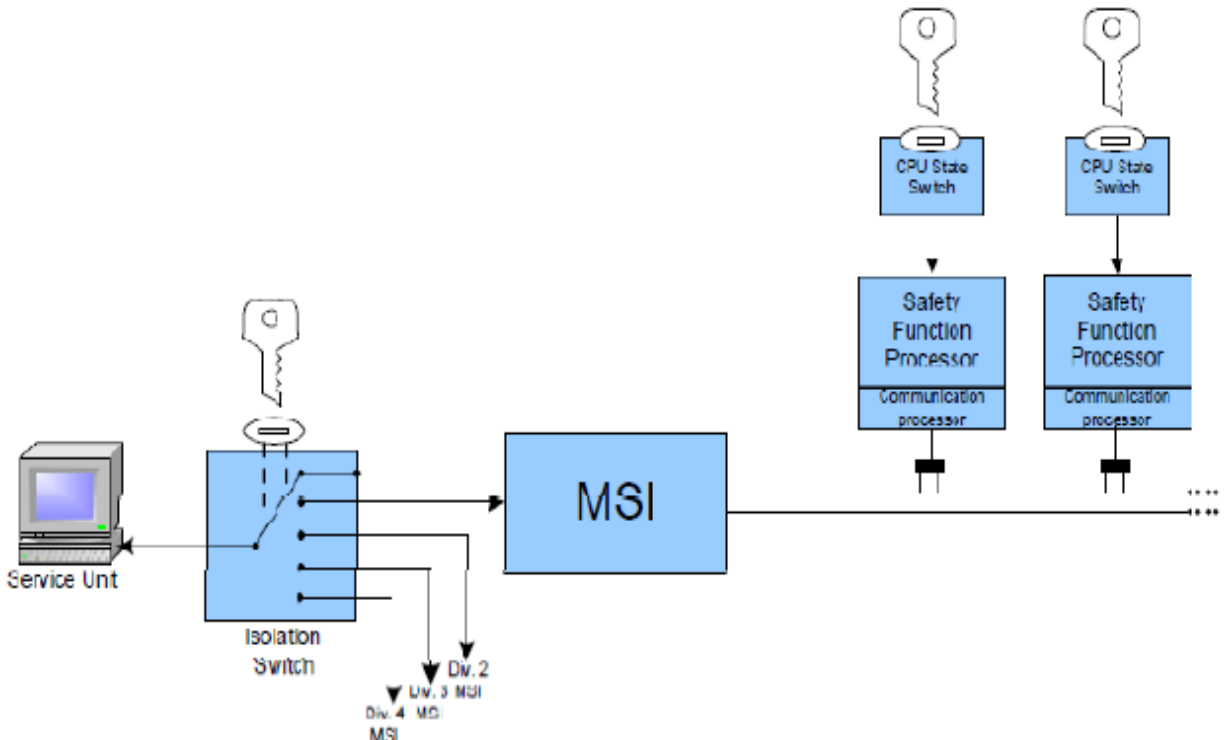
##### 7.1.4.16.1 *Service Unit*

The SU is a non-safety-related computer that is temporarily connected to various TXS-based I&C systems. The SU provides the hardware and software necessary for the performance of periodic testing and maintenance activities (i.e., fault diagnostics and troubleshooting) and is the primary user interface to perform these activities in the U.S. EPR design. The applicant did not specifically state in FSAR Tier 2, Section 7.1 which I&C systems utilized a SU. Based upon a review of the figures provided in FSAR Tier 2, Section 7.1, safety related PS, SAS and RPMS each utilize the SU. A description of the SU design and implementation is provided in FSAR Tier 2, Section 7.1.1.6.4. Figure 7.1-1 below illustrates the SU connection.

The functions the SU performs includes the following:

- Reading/acknowledging online error and state messages

- Modifying online parameters
- Performing surveillance testing
- Performing non-Technical Specification maintenance activities
- Troubleshooting and fault diagnostic
- Loading software



**Figure 7.1-1 Service Unit Implementation in U.S. EPR**

[Source: Figure 7.1-6 and Figure 7.1-7 of FSAR Tier 2, Section 7.1]

The SU connection incorporates two switches:

- **Hardwired Disconnect Switch:** Each division for PS and SAS has a hardwired disconnect/connection switch. This switch establishes the physical connection between the SU and one of the four MSIs of each division of PS or SAS. This is added to ensure the SU is connected to only one division at a time. The hardwired disconnect switch is the credited independence mechanism for the SU configuration as per guidance from DI&C-ISG-04, Position 1, Point 10. The SU connection is located in the I&C service center.
- **CPU State Switch:** Each function processor has a CPU state switch for PS and SAS. The CPU state switch is key-operated. Turning the CPU state switch enables the operator at the SU to change the operating state of the desired function processor. The CPU state switch's intended purpose is to prevent unintended alteration of

modifiable parameters and software via the SU while it is connected. These switches are located in the associated function processor's TXS cabinet.

FSAR Tier 2, Section 7.1 states that the SU will only be temporarily connected for the following three reasons:

1. Performing Technical Specification Surveillance Requirements and associated actions
2. Diagnosing system faults following indication of a fault
3. Loading new software versions needed to implement approved plant design changes

FSAR Tier 2, interim Revision 3 mark-ups, Table 7.1-6, "Function Processor Operational States," describes the function processor operational states during SU operation. Based on a review of available documentation, the staff found there was insufficient detail concerning the implementation of the SU design into the various TXS safety I&C systems. Therefore, in RAI 485, Question 07.09-70, the staff requested that the applicant provide further clarification. In a June 22, 2011 response to RAI 485, Question 07.09-70, the applicant provided information on the operating modes of the TXS function processor, matching specific surveillance tests to the function processor operating modes that would be performed, and an estimated amount of time the SU would need to be plugged into a division to perform various surveillance activities.

After reviewing the applicant's June 22, 2011 response to RAI 485, Question 07.09-70, the staff has the following concerns:

- The June 22, 2011 response to RAI 485, Question 07.09-70, is not complete. The staff understands that certain surveillance tests, such as the No-Go actuating device operational test, as documented in Technical Report ANP-10315P, are required to be performed in both cyclic processing and parameterization TXS processor states. With RAI 485, Question 07.09-70, the staff specifically requested the applicant map each I&C surveillance test to the function processor operating state for which the surveillance would be performed. Multi-state surveillance information was not included as part of the applicant's response and the staff considers the applicant's response to RAI 485, Question 07.09-70 incomplete. This information is also not available in Technical Report ANP-10315P, Revision 1.
- Based on a review of the applicant's June 22, 2011 response to RAI 485, Question 07.09-70, it is not clear how operability is addressed in multi-state surveillance tests. The applicant considers a TXS function processor operable in cyclic processing state. The applicant considers a function processor inoperable for all other TXS processor states. It is not clear in the applicant's response, or in other available design documentation, how operability would be addressed for multi-state situations.
- In terms of parameterization and function test processor states, the TXS function processor outputs remain active while the function processor is considered inoperable by the applicant in both states. According to the applicant's June 22, 2011 response to RAI 485, Question 07.09-70, all outputs remain fully active in parameterization state. For the functional test state, hardwired outputs are set to zero, but data messages are still actively transmitted and processed by receiving CPUs that are also in the functional test state.

The staff determined that the June 22, 2011 response to RAI 485, Question 07.09-70, as well as other available design information, does not provide a clear and complete understanding of the implementation of the SU, including effects on equipment function and operability while the SU is in use. Therefore, in follow-up RAI 505, Question 07.01-51, the staff requested that the applicant address these issues. **RAI 505, Question 07.01-51 is being tracked as an open item.**

#### 7.1.4.17 *Derivation of System Inputs*

The staff reviewed the application to verify that IEEE Std 603-1998, Clause 6.4, has been appropriately addressed. IEEE Std 603-1998, Clause 6.4 requires, in part, that sense and command features of the PS be direct measures of specified process variables shown in the design basis, when practical. In other words, to minimize the number of variables or derivatives of direct measured variables and secondary calculations required to provide the required measurement. The staff used SRP Appendix 7.1-C as guidance for this area of the evaluation.

In FSAR Tier 2, Section 7.1.2.6.31, "Derivation of System Inputs (Clause 6.4)," the applicant states that all signals used in the sense and command features are direct measures of the desired variable used in the design basis. The staff reviewed the measured variables documented in FSAR Tier 2, Section 7.2 and Section 7.3, and confirmed that system inputs, are, to the extent feasible and practical, derived from signals that are direct measures of the desired variables. Based on the identification of the necessary design requirement, the staff's review of the design, and the verification of the design requirements in the ITAAC, the staff finds that Clause 6.4 has been adequately addressed.

#### 7.1.4.18 *Multi-Unit Stations*

The staff reviewed the application to verify whether IEEE Std 603-1998, Clause 5.13 has been adequately addressed for the U.S. EPR safety systems. IEEE Std 603-1998, Clause 5.13 allows sharing of SSCs between units at multi-unit generating stations provided that the ability to simultaneously perform required safety functions in all units is not impaired.

FSAR Tier 2, Section 7.1.2.6.24, "Multi-Unit Stations (Clause 5.13)," states that the safety systems meet the requirements of IEEE Std 603-1998, Clause 5.13 as the U.S. EPR is a single-unit plant design. If multiple units are constructed at the same site, safety systems are not shared between sites. Since there is no shared safety system among multiple units, the ability to simultaneously perform required safety functions in all units is maintained. Based on the commitment that no safety systems are shared between multiple U.S. EPR units, the staff finds that IEEE Std 603-1998, Clause 5.13 has been adequately addressed.

#### 7.1.4.19 *Human Factors Considerations*

IEEE Std 603-1998, Clause 5.14 requires, in part, that human factors be considered throughout the design process. FSAR Tier 2, Section 7.1.2.6.25, "Human Factors Considerations (Clause 5.14)," states that this requirement is met, because human factors are considered throughout the design of the safety systems FSAR Tier 2, Chapter 18 also discusses the human factors engineering associated with the U.S. EPR design. **Upon satisfactory resolution of open items in Chapter 18 of this report, the staff should be able to find that the U.S. EPR design meets IEEE Std 603-1998, Clause 5.14.**

#### 7.1.4.20 *Reliability*

The requirement of IEEE-603-1998, Clause 5.15, states that for the systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. GDC 29 requires that the protection and reactivity control systems be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences. Guidance on the application of this criterion for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.

FSAR Tier 2, Section 19.1.1.1, "Design Phase," Revision 2, states that the use of the probabilistic risk assessment through the design phase was to determine how the risk associated with the design compares against the quantitative objectives established by the Commission that the core damage frequency is less than  $1.0\text{E-}04/\text{yr}$ , and the large release frequency should be less than  $1.0\text{E-}06/\text{yr}$ . FSAR Tier 2, Section 19.1.4.1.2.1, "Risk Metrics," Revision 2, states that the total Level 1 core damage frequency from internal events is  $2.8\text{E-}07/\text{yr}$  which is less than the NRC goal of  $1\text{E-}04/\text{yr}$ . FSAR Tier 2, Section 19.1.4.2.2.1, "Risk Metrics (LRF, CCFP)," Revision 2, states that total large release frequency (LRF) from Level 2 internal events is  $2.2\text{E-}08/\text{yr}$ , which is less than NRC goal of  $1\text{E-}06/\text{yr}$ .

SRP Appendix 7.1-D indicates that the concept of quantitative reliability goals is not sufficient as a sole means of meeting the NRC regulations for the reliability of digital computers used in safety systems. The assessment of reliability should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures. Hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Software failure conditions to be considered should include, as appropriate, software common-cause failures, cascading failures, and undetected failures

FSAR Tier 2, Section 7.1.2.6.26, "Reliability (Clause 5.15)," Interim Revision 3 mark-ups, states that safety-related systems meet the requirements of IEEE Std 603-1998 and the additional guidance of IEEE Std 7-4.3.2-2003 to support overall plant availability. The applicant states that high reliability is provided through redundant architecture, reliable equipment, independent PS subsystems, continuous online fault detection, high quality software design process, and operating experience of the TXS platform. The safety systems (including software) are analyzed as part of the probabilistic risk assessment, which is described in FSAR Tier 2, Chapter 19, "Probabilistic Risk Assessment and Severe Accident Evaluation." In RAI 75, Question 07.02-17, the staff requested that the applicant clarify hardware and software failures and how they are addressed in FSAR Tier 2, Section 7.1.2.6.26. In a June 12, 2009 response to RAI 75, Question 07.02-17, the applicant provided information explaining the effects of possible hardware and software failures, as well as design features that have been incorporated to prevent or limit effects of failures. In a March 31, 2009 response to RAI 75, Question 07.02-17, the applicant also addressed the reliability issue raised in this RAI from the following four design features for the U.S. EPR design certification application. The first design feature is that the worst-case single, credible hardware and software failures in an I&C safety system will not result in the loss of the safety function. Several functions have been incorporated to prevent the loss of a safety function due to the effects of hardware and software failures. One of these features is the highly redundant architecture design. Each safety I&C system has four redundant and independent divisions so that a single software or hardware failure does not result in the loss of a safety function. The second design feature which prevents or limits the effects of hardware and software failures is the use of a high quality

software development process. The software development process is in accordance with SRP BTP 7-14 to increase the reliability of the software produced and therefore reduce the probability of hardware and software failures. The third design feature is that the safety I&C systems are implemented using the TXS digital platform. The TXS platform includes design features that limit the effects of failures, such as the continuous online self testing and diagnostics that allow early detection of hardware and software failures. The last design feature is the use of a platform diverse from TXS that can be used to automatically initiate required safety functions, or allow manual execution of required safety functions by the operator in the event that a SCCF occurs. Despite the high quality of design and the use of defensive measures to combat hardware and software system failures, it is still possible that a software failure may defeat the safety functions in redundant safety divisions through a SCCF. This diverse system is the DAS, and its functions are described in FSAR Tier 2, Section 7.8, "Diverse I&C Systems." The staff reviewed the applicant's March 31, 2009, response to RAI 75, Question 07.02-17 and finds that the applicant addressed the issues raised in the RAI. The staff finds the applicant meets the requirement of Clause 5.15 of IEEE Std 603-1998 and GDC 29 by providing the above deterministic design features and processes in the U.S. EPR safety-related systems.

The staff's evaluation of the U.S. EPR data communication systems reliability is included in Section 7.9 of this report.

#### 7.1.4.21 *Diversity and Defense-in-Depth*

Except for the PACS discussion below, the staff evaluation on how the applicant addressed software common cause failure is discussed in Section 7.8 of this report.

##### 7.1.4.21.1 *PACS Diversity and Defense-in-Depth*

IEEE Std 603-1998, Clause 5.16 requires, in part, that plant parameters shall be maintained within acceptable limits established for each DBE in the presence of a single CCF. In addition, 10 CFR Part 50, Appendix A, GDC 22 requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation be used to the extent practical to prevent loss of the protective function. DI&C ISG 02, Section 5, Point 2 provides guidance for consideration of an SCCF. As stated, "The design attributes of sufficient diversity and testability can be used to eliminate consideration of CCF." The applicant submitted Technical Report ANP-10310, "Methodology for 100% Combinatorial Testing of the U.S. EPR™ Priority Module Technical Report," Revision 1, which presents an example of 100 percent combinatorial testing of a PACS priority module. FSAR Tier 1, Section 2.4.10, Interim Revision 3 Mark-Ups, states that the capability of 100 percent combinatorial testing of the PACS priority module is provided to preclude a SCCF failure. FSAR Tier 2, Section 7.1.1.4.3, states that the priority module must be 100 percent tested to eliminate consideration of SCCF.

In Technical Report ANP-10310P the applicant provided a methodology for 100 percent combinatorial testing and manual verification, which provides quality assurance and addresses the likelihood of a SCCF in the design implementation phase of the PACS. However, the 100 percent combination testing would not address potential design faults that may be introduced in the requirements specification or design specification phases of the PACS development lifecycle. In RAI 373, Question 07.01-25, the staff requested that the applicant provide additional information regarding the requirements V&V and the timing analysis to address the potential for software common cause faults in the requirements and design

specification phases of the PACS development. In a December 3, 2010 response to RAI 373, Question 07.01-25, the applicant's response stated that the PACS's priority module is safety-related and designed under the TXS quality assurance (QA) program as described in Topical Report EMF-2110. The staff's review of safety evaluation for Topical Report EMF-2110 finds that the TXS software development process met the quality requirements of IEEE Std 603-1991. Further discussion of the staff's review of the PACS 100 percent combinatorial testing is discussed in Section 7.1.4.7 of this report. As a result of the applicant's commitments regarding 100 percent combinatorial testing of the PACS safety logic, the staff finds that the applicant appropriately does not need to consider a SCCF of the PACS. Based on the commitments for 100 percent combinatorial testing, the staff finds the PACS design meets IEEE Std 603-1998, Clause 5.16 and GDC 22.

#### *7.1.4.22 Automatic and Manual Control*

##### *7.1.4.22.1 Protection System Controls*

The staff reviewed U.S. EPR design certification application to verify that IEEE Std 603-1998, Clauses 6.1 and 7.1, and GDC 20, have been adequately addressed. IEEE Std 603-1998, Clause 7.1 requires that capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with IEEE Std 603-1998, Clause 4d of the design basis. IEEE Std 603-1998, Clause 6.1 requires that means shall be provided to automatically initiate and control all protective actions except as justified in IEEE Std 603-1998, Clause 4e. GDC 20 requires the protection system to be designed to initiate automatically the operation of appropriate systems including the reactivity control systems to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and to sense accident conditions and to initiate the operation of systems and components important to safety. SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 7.1 states that the applicant's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements, except as justified in IEEE Std 603-1991, Clause 4.5, are met and that the analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The guidance of SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 6.1 indicates that the applicant's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met, and that the evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis.

- FSAR Tier 2, Section 7.1.2.6.28, states that safety systems meet the requirements of IEEE Std 603-1998, Clauses 6.1 and 7.1, and that PS is designed to automatically initiate reactor trip and actuate the ESF systems necessary to mitigate the effects of DBEs. The applicant incorporated the following design aspects into the U.S. EPR design:
- An approved setpoint methodology for the FSAR.
- Operating margins for process variables monitored for RT and ESFAS presented in FSAR Tier 2, Sections 7.2 and 7.3.
- The safety analytical limit and corresponding system response times (time delays) for each RT and ESF function documented in FSAR Tier 2, Tables 15.0-7 and 15.0-8, respectively.



- ITAAC Item 4.1 and 4.2 from FSAR Tier 1, Table 2.4.1-7, which verifies the completion of protective action for automatic ESF actuation signals.

The setpoint methodology for the U.S. EPR design was approved by the staff and documented in Topical Report ANP-10275P "U.S. EPR Instrument Setpoint Methodology Topical Report," Revision 0. FSAR Tier 2, Section 7.3.1.2, describes how each ESF function is designed to initiate an automatic protective action based upon plant conditions. For each ESF function, the plant condition, and process variable range is given for the automatic actuations on FSAR Tier 2, Table 7.3-1. Setpoints and response times (time delays) are documented in the accident analyses for each ESF function. FSAR Tier 1, Table 2.4.1-7, ITAAC Item 4.2 performs the verification of completion of protective action for each ESF function. The test verifies that upon reception of a demand signal, the corresponding ESF function will actuate to completion, subsequently requiring operator action to reset the system. ITAAC Item 4.6 performs a verification of the methodology and efficacy of ESF setpoints. ITAAC Item 4.24 performs a verification of the response times for ESF signals.

Per guidance from SRP BTP 7-21, the applicant provided a reliable and precise method for ensuring automatic actuation for specified RT and ESF actuations. The RT and ESF response times account for all I&C timing delays involved in an instrument channel from sensor to final actuation device. These design aspects ensure that the RT and ESF automatic actuations have an acceptable level of determinism with predictable performance margins when a demand signal is present. Therefore, the staff finds the U.S. EPR design meets the requirements of GDC 20 and IEEE Std 603-1998, Clauses 6.1 and 7.1.

FSAR Tier 1, Table 2.4.1-7, ITAAC Item 4.24 performs the verification of PS response times. FSAR Tier 2, Table 15.0-8, Note 4 regarding Time Delay (response times) states:

Represent the total time for completion of the function. Includes sensor delay, I&C delay (includes PS computerized portion, and PACS delays), and other delays as noted until the function is completed.

The individual PACS modules are all downstream of the ALUs in all four PS divisions, as represented by FSAR Tier 2, Figure 7.3-1. As it is currently worded, ITAAC Item 4.24 would not adequately verify the response time requirement of the accident analyses because the test does not incorporate all timing delays if the test measurement ends at the output of the individual ALUs. Therefore, in RAI 505, Question 07.01-47, the staff requested that the applicant address this issue. **RAI 505, Question 07.01-47 is being tracked as an open item.**

The staff reviewed the FSAR to verify that IEEE Std 603-1998, Clause 6.2 and Clause 7.2 have been adequately addressed. IEEE Std 603-1998, Clause 6.2 requires, in part, that means be provided to manually initiate protective system actuation at the division level with minimal number of discrete operator manipulations. Similarly, Clause 7.2 requires, in part, that any additional design features in the execute features necessary to accomplish manual controls shall not defeat single failure protection and will support the capability of other safety-related manual controls. The applicant addresses compliance with IEEE Std 603-1998, Clauses 6.2 and 7.2 in FSAR Tier 2, Section 7.1.2.6.29. The staff used SRP Appendix 7.1-C as guidance for this area of the evaluation, which references RG 1.62 as an acceptable means of addressing compliance with IEEE Std 603-1998, Clause 6.2 and Clause 7.2. Compliance with the requirements of IEEE Std 603-1998, Clause 6.2 and Clause 7.2 are documented in FSAR Tier 2, Section 7.1.2.6.29.

IEEE Std 603-1998, Clause 6.2.a states that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment in conformance with the constraints of IEEE Std 603-1998, Clause 5.6.1. FSAR Tier 2, Sections 7.2.1.1 and 7.2.1.2.22, "Manual Reactor Trip," state that the operator is able to manually trip the reactor through the SICS from either the MCR or RSS. In the MCR and RSS, four manual RT buttons are provided in each location to the four PS divisions. In RAI 413, Question 07.02-33, the staff requested that the applicant clarify how many buttons are required to manually actuate an RT. In a February 3, 2011, response to RAI 414, Question 07.02-33, the applicant stated that any two of these four buttons together will actuate an RT. Each button is wired directly into the hardwired logic for trip actuation that bypasses the electronics of the PS, and also each button is hardwired to a digital input card on each ALU in the corresponding division so that either an automatic function or manual command sets the RT outputs of the ALU. In both of these configurations, the manual RT from the MCR or RSS acts on the same RT devices as the PS automatic RT functions. The manual reactor trip acts directly on the under-voltage coils of the RT breakers. FSAR Tier 2, Figure 7.2-4, shows the logic diagram for the RT breakers and RT contactors. The RT breakers are arranged in a "1 out of 2 taken twice" and requires the following logical combination of PS divisional RT orders to actuate an RT: (1 or 2) and (3 or 4). With this RT breaker logic, pressing two buttons corresponding either to Divisions 1 and 2 or to Divisions 3 and 4 will not result in an RT by the RT breakers. However, since RT contactors are arranged in a two-out-of-four configuration, an RT order issued from any two PS divisions will result in an RT. Additionally, the execute feature for the RT is the RT breakers and contactors. These components are redundant and independent on a divisional basis in order to provide single failure protection. The RT breakers and contactors are designed to receive the division-level RT signal and execute the RT function.

Design information concerning ESF manual controls are described in FSAR Tier 2, Section 7.3. For ESF, both system-level and component-level controls are available to the operator. System-level manual controls are available on the SICS, which is located in the MCR. System-level manual controls corresponding to each ESF function are described in FSAR Tier 2, Section 7.3.1.2. System-level manual controls are acquired by the ALUs and combined with the automatic actuation logic, as shown in FSAR Tier 2, Figure 7.3-1, Sheet 2. Component-level manual controls are available to the operator on both the SICS and PICS. Both of these panels are located in the MCR. Commands from the SICS are sent directly to the PACS for prioritization. Commands from the PICS are processed by PAS and then sent to the PACS for prioritization. Manual reset of sense and command ESF actuation outputs are available on the SICS. FSAR Tier 2, Section 7.1.2.6.29, states that manual control signals are lower in priority than the automatic actuation signals in the PS. The execute features include the necessary pumps, valves, breakers, and fans for each respective ESF function. These components are redundant and independent on a divisional basis in order to provide single failure protection, and they are designed to receive the division- and component-level manual commands and act upon them.

RG 1.62 provides six regulatory positions for addressing manual controls design. Table 7.1-2 below provides a summary of the regulatory positions and the U.S. EPR conformance the regulatory positions. Upon completion of the open item identified in Table 7.1-2, the staff finds the U.S. EPR design meets the requirements of IEEE Std 603-1998, Clauses 6.2 and 7.2.

**Table 7.1-2 Conformance to RG 1.62 Regulatory Positions**

RG 1.62 Manual Controls Criteria <sup>1</sup>	US EPR Design Information	Verified by ITAAC – Table 2.4.1-7
Position 1 - Means should be provided for the manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve).	Tier2, Section 7.3.1.2, documents the corresponding system-level manual control capability for each automatic ESF actuation. Each system-level control is available to the operator in the MCR.	Verified by ITAAC Item 4.11
Position 2 - Manual initiation of a protective action on a division-level basis should perform all actions performed by automatic initiation, such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to ensure correct valve position, and providing the credited action-sequencing functions and interlocks.	FSAR Tier 2, Section 7.3.1.2, documents the corresponding system-level manual control capability for each automatic ESF actuation. Manual system-level control signals are acquired by divisional ALUs and combined with automatic actuation logic, ensuring that manual commands perform the same functions as the automatic commands.	Verified by ITAAC Item 4.11
Position 3 - The control interfaces for manual initiation of protective actions on a division-level basis should be located in the control room. They should be easily accessible to the operator so that action can be taken in an expeditious manner at the point in time or under the plant conditions for which the protective actions of the safety system shall be initiated, as required in Section 4.10.1 of IEEE Std 603-1991. Information displays associated with manual controls should (i) be readily present during the time that manual actuation is	FSAR Tier 2, Section 7.3, states that manual system-level controls for ESF actuation exist on the SICS, which resides in the MCR.	Verified by ITAAC Item 4.11

RG 1.62 Manual Controls Criteria1	US EPR Design Information	Verified by ITAAC – Table 2.4.1-7
necessary, (ii) be visible from the location of the manual controls, and (iii) provide unambiguous indications that will not confuse the operator.		
Position 4 - No single failure within the manual, automatic, or common portions of the protection system should prevent initiation of a protective action by manual or automatic means.	<p>The PS is divided into four separate, redundant divisions, which includes, dedicated divisional manual controls as well. Per Technical Report ANP-10309P, Section 5.2, the manual system-level actuation is a hardwired path from SICS to each ALU in a division. There are four ALUs in each PS division. The system-level manual control signals are independent of automatic actuation logic processing in a division.</p> <p>Failures of this type would be bounded by overall single failure analysis for an entire PS division. The PS FMEA is documented in Technical Report ANP-10309P, Appendix A.</p>	Verified by ITAAC Item 4.18
Position 5 - Manual initiation of protective actions should depend on the operation of a minimum amount of equipment, consistent with Positions 1, 2, 3, and 4 above.	<p>Per FSAR Tier 2, Figure 7.3-1, Sheet 2 of 5, the manual system-level control appears to be a push-button or switch. There is no drawing key available in FSAR Tier 2, Sections 7.1 or 7.3, to provide a definitive answer. The manual system-level commands are hardwired between the SICS and ALUs, which suggests a minimal amount of equipment utilized to perform these actions. Manual system-level control logic is shown on FSAR Tier 2 Figure 7.3-1, Sheet 2 of 5. The manual system-level commands are hardwired between the SICS</p>	N/A

RG 1.62 Manual Controls Criteria1	US EPR Design Information	Verified by ITAAC – Table 2.4.1-7
	and ALUs, which minimizes the amount of equipment necessary to perform these actions.	
Position 6 - Manual initiation of a protective action on a division-level basis should be designed so that, once initiated, the action will go to completion, as required in Section 5.2 of IEEE Std 603-1991.	FSAR Tier 2, Section 7.3.1.2, documents the corresponding system-level manual control capability for each automatic ESF actuation.	Refer to Section 14.3.5.4.1 of this report. ITAAC Item 4.11 provides for the verification of manual system-level controls. The acceptance criteria for ITAAC Item 4.11 do not present the level of detail similar to that of ITAAC Item 4.2, which addresses Clause 5.2 (Completion of Protective Action) for automatic actuations. It is not clear that ITAAC Item 4.11 verifies that the manual actuation sequence goes on to completion before reset. This is considered an <b>open item being tracked by RAI 506, Question 14.03.05-42.</b>

Note: For this portion of the evaluation, 'division-level' will be considered synonymous with 'system-level'.

For the SGTR event, the system-level manual controls are the credited means of accident mitigation as described in Chapter 15, "Transient and Accident Analyses." These controls are the only credited manual controls in the FSAR. Clause 6.2.2 requires, in part, the implementation of manual controls for those protective actions that automatic controls have not been selected. The applicant identified in interim revision 3 of FSAR Tier 2, Section 7.3 the ESF systems for which the manual system-level actuation and controls are credited means of system initiation. For each ESF system related to mitigation of the SGTR event, the applicant stated in each sub-section that it is the manual system-level controls credited for the ESF actuation, and those controls for each ESF system are available on the SICS, which is the safety-related control and display panel. The staff finds the requirements of Clause 6.2.2 have been adequately addressed based on the identification of credited manual system-level controls for specified ESF systems and the availability of these controls on SICS.

As described above, the U.S. EPR I&C design meets IEEE Std 603-1998, Clause 6.2 by conforming to the guidance of RG 1.62. Specifically, division-level manual actuation capability is provided with a minimum of operator manipulations, safety-related manual controls and indications are provided for credited operator actions described in FSAR Tier 2, Chapter 15, and appropriate manual controls and indications are provided to achieve safe shutdown. The U.S. EPR I&C design meets IEEE Std 603-1998, Clause 7.2 since the execute features receive and

act upon division- and component-level manual commands and maintain single failure protection.

#### *7.1.4.22.2 SAS Controls*

FSAR Tier 2, Section 7.1.2.6.28, addresses IEEE Std 603-1998, Clauses 6.1 and 7.1. The applicant states that the safety systems are designed to meet the requirements of IEEE Std 603-1998, Clauses 6.1 and 7.1. FSAR Tier 1, Section 2.4.4, states that the SAS receives input signals from systems listed in FSAR Tier 1, Table 2.4.4-2, and provides output signals to systems listed in FSAR Tier 1, Table 2.4.4-3. FSAR Tier 1, Table 2.4.4.2, lists the systems that provide the initiating conditions for SAS. FSAR Tier 1, Table 2.4.4-3, lists systems for which SAS provides automatic controls. ITAAC Items 4.3 and 4.4 on FSAR Tier 1, Table 2.4.4-6, verify this design information.

In the staff's review of the SAS automatic controls, it was unclear if the SAS functions had certain timing requirements. For example, if SAS addresses safety functions in the accident analysis that may have timing requirements, how are these requirements addressed? Therefore, in RAI 505, Question 07.01-48, the staff requested that the applicant address this issue. **RAI 505, Question 07.01-48 is being tracked as an open item.**

FSAR Tier 2, Section 7.1.2.6.29, addresses IEEE Std 603-1998, Clauses 6.2 and 7.2. The applicant states that the safety systems are designed to meet the requirements of IEEE Std 603-1998, Clauses 6.2 and 7.2. FSAR Tier 1, Section 2.4.4, does not provide any information regarding SAS manual controls. FSAR Tier 2, Section 7.1.1.4.2, states that SAS can perform manual 'grouped' commands. There is also no information in the ITAAC verifying where SAS controls and displays are located and verifying if they're in the MCR, specifically on the SICS. Also, the ITAAC does not verify the design functionality of the manual grouped controls for SAS. FSAR Tier 2, Table 7.1-4, states that the SICS has a hardwired connection to the SAS for manual grouped commands, so this is also a potential discrepancy in FSAR Tier 1 information. Therefore, in RAI 505, Question 07.01-48, the staff requested that the applicant address this issue. **RAI 505, Question 07.01-48 is being tracked as an open item.**

#### *7.1.4.22.3 SICS Controls*

FSAR Tier 2, Section 7.1.2.6.29, addresses IEEE Std 603-1998, Clauses 6.2 and 7.2. The applicant states that the safety systems are designed to meet the requirements of IEEE Std 603-1998, Clauses 6.2 and 7.2.

FSAR Tier 2, Section 7.1.2.6.29, states that manual actuation of protective actions are available at the division level on the SICS. The applicant states this method of implementation minimizes the amount of discrete operator manipulations, and depends on a minimum of equipment. The applicant states the following in FSAR Tier 2, Section 7.1, Interim Revision 3 mark-ups:

During normal operation, the operational I&C disable switch on the SICS is set so that the PAS can send commands to the PACS. In this configuration, automatic commands from the PAS override manual commands from the SICS because of the nature of the manual control logic in the PACS. If the operational I&C disable switch is set to DISABLE by the operator, the PAS input will be disabled (i.e., the input signals from the PAS to the communication module will be blocked from being sent to the priority module), providing the priority of the SICS manual commands. The operational I&C disable switch disables PAS inputs, all other PACS inputs remain operational.

The staff considers this an issue for the U.S. EPR design, considering that manual, system-level controls on the SICs are the credited means for the operators to mitigate the SGTR event. A failure of the switch, or a failure of the operator to use the disable switch during an event could have unforeseen consequences for plant safety and operations. Therefore, in RAI 505, Question 07.01-46, the staff requested that the applicant provide additional information on the operation of the I&C disable switch. Specifically, the staff requested that the applicant identify if the switch is safety-related, and if so, how it meets the requirements such as those for single failure protection. **RAI 505, Question 07.01-46 is being tracked as an open item.**

#### *7.1.4.23 Operating Bypasses*

##### *7.1.4.23.1 PS Operating Bypasses*

The staff reviewed the application to determine whether IEEE Std 603-1998, Clause 6.6 has been adequately addressed. These requirements state, in part, that whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). The operator may take action to prevent the unnecessary initiation of a protective action. SRP Appendix 7.1-C states that the requirement for automatic removal of operational bypasses means that reactor operator action shall not be required.

FSAR Tier 2, Section 7.1.2.6.33 states that safety systems meet the requirements of IEEE Std 603-1998, Clause 6.6 and 7.4, and that operating bypasses are implemented using permissive signals from the PS. The applicant indicates that if the plant conditions associated with allowing operational bypasses are not met, the PS automatically prevents the activation of the operating bypass. If plant conditions change during activation of an operating bypass, and the operating bypass is no longer permissible, the PS automatically removes the appropriate active operating bypass or automatically initiates the appropriate safety function. The staff finds that IEEE Std 603-1998, Clauses 6.6 and 7.4 have been met by the commitments above.

##### *7.1.4.23.2 SAS Operating Bypasses*

The staff reviewed the application to determine whether IEEE Std 603-1998, Clause 6.6 has been adequately addressed. In a June 12, 2009, response to RAI 78, Question 14.03.05-4, which addressed operating bypass functionality, the applicant identified that operating bypass functionality for SAS is verified by ITAAC Item 4.3 in FSAR Tier 1, Table 2.4.1-7. Table 2.4.1-7 is the FSAR Tier 1 ITAAC table for the PS. The PS has limited interaction with SAS. SAS contains a significant number of continuous functions that are outside the bounds of its interaction with the PS, and therefore would not be verified by ITAAC Item 4.3. The staff is unclear as to operating bypasses of the SAS. Therefore, in follow-up RAI 505, Question 07.01-49, the staff requested that the applicant address this issue. **RAI 505, Question 07.01-49 is being tracked as an open item.**

#### *7.1.4.24 Maintenance Bypasses*

##### *7.1.4.24.1 PS Maintenance Bypasses*

The staff reviewed the application to determine whether IEEE Std 603-1998, Clauses 6.7 and 7.5, have been adequately addressed. These requirements state, in part, that the capability of a safety system to accomplish its safety function shall be retained while sense and command and execute features equipment is in maintenance bypass. During such operation, the features

shall continue to meet the requirements of IEEE Std 603-1998, Clauses 5.1 and 6.3. The guidance of SRP Appendix 7.1-C states that the review of bypass and removal from operations requirements should be coordinated with the organization responsible for reviewing Technical Specification format and content to confirm that the provisions for this bypass are consistent with the required actions of the proposed plant Technical Specifications.

FSAR Tier 2, Section 7.1.2.6.34, states that the safety systems meet the requirements of IEEE Std 603-1998, Clauses 6.7 and 7.5, in that the safety systems are designed to permit channel bypass for maintenance, testing or repair. The initial application did not adequately address how the PS ITAAC will test and verify to assure compliance with IEEE Std 603-1998, Clauses 6.7 and 7.5. The staff reviewed FSAR Tier 2, Sections 7.1 and 7.3 of the application and finds that these requirements are not adequately addressed by the design. In RAI 75, Questions 07.02-22 and 07.02-24, the staff requested that the applicant address this issue. In the November 3, 2008 responses to RAI 75, 07.02-24, the applicant added a clause to Tier 2 Section 7.1.2.6.34, stating that “sufficient redundancy and administrative controls that manage reduction of redundancy exist within each system to maintain acceptable reliability when a portion of the execute features is placed in bypass, in accordance with IEEE 603-1998, Clause 7.5.” Tier 2 Section 7.1.2.6.34 additionally states “the safety-related systems meet the requirements of Clause 6.7 of IEEE Std 603-1998.” The staff finds that these statements are sufficient to ensure that IEEE Std 603-1998, Clauses 6.7 and 7.5 are adequately addressed in the design. In the June 12, 2009 response to RAI 75, Question 07.02-22 the applicant asserted that Tier 1 Table 2.4.1-7 Item 4.5 adequately verifies compliance with IEEE Std 603-1998, Clauses 6.7 and 7.5. This commitment states “The PS is capable of performing its safety function when PS equipment is in maintenance bypass. Bypassed PS equipment is indicated in the MCR.” The staff finds that this commitment and the ITAAC of Tier 1 Table 2.4.1-7 Item 4.5 are sufficient to verify compliance with IEEE Std 603-1998, Clauses 6.7 and 7.5. Additional discussion of the staff review of this issue is provided in Sections 7.2, 7.3, and 14.3.5 of this report. The staff finds that the design meets IEEE Std 603-1998, Clauses 6.7 and 7.5.

#### *7.1.4.24.2 SAS Maintenance Bypasses*

The staff did not find any design information in FSAR Tier 2, Section 7.1.1.4.2, concerning SAS maintenance bypass functionality. In FSAR Tier 2, Section 7.1.2.6.34, the applicant states that safety systems are designed to permit channel bypass for maintenance, testing or repair. The applicant also states that during the maintenance bypass, single failure criterion is still met or acceptable reliability is demonstrated. In terms of SAS functionality, the applicant has not provided sufficient design information for the staff to determine how SAS meets IEEE Std 603-1998, Clause 5.1. Specifically, the applicant has not provided a SAS FMEA, or other single failure analysis, toward this conclusion. The applicant also did not provide FSAR Tier 1 design information concerning SAS maintenance bypass functionality. In RAI 505, Question 07.01-49, the staff requested that the applicant address the single failure protection, along with maintenance bypass for SAS. **RAI 505, Question 07.01-49 is being tracked as an open item.**

#### *7.1.4.25 Setpoints*

The staff reviewed the application to determine whether IEEE Std 603-1998, Clause 6.8 has been adequately addressed. IEEE Std 603-1998, Clause 6.8 states, in part, that the allowance for uncertainties between the process analytical limit documented in IEEE Std 603-1998, Clause 4.d and the device setpoint shall be determined using a documented methodology. IEEE Std 603-1998, Clause 4.d requires, in part, the identification of the analytical limit



associated with each variable. IEEE Std 603-1998, Clause 6.8 also states that where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. Where it is necessary to provide multiple setpoints as discussed in IEEE Std 603-1998, Clause 6.8, the staff's interpretation of "positive means" is that automatic action is provided to ensure that the more restrictive setpoint is used when required. SRP BTP 7-3 provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

FSAR Tier 2, Section 7.1.2.6.35, states that the U.S. EPR I&C safety systems meet the requirements of IEEE Std 603-1998, Clause 6.8, and that allowance for uncertainties between the process analytical limit and the setpoint used in the protective functions of the PS is determined using a methodology as documented in the Topical Report ANP-10275P. The staff reviewed this topical report and found that it is acceptable for referencing in licensing applications for U.S. EPR to the extent specified and under limitations delineated in the topical report and its associated safety evaluation

FSAR Tier 2, Sections 7.2.2.3.7 and 7.3.2.3.8, state, in part, that each setpoint used to initiate an RT function or actuate an ESF system is selected based on the safety limits assumed in the plant accident analysis. Each RT and ESF setpoint provides margin to the safety limit and takes into account measurement uncertainties. The methodology to determine setpoints used in SPND-based RT functions is documented in Topical Report ANP 10287P, "In-core Trip Setpoint and Transient Methodology for U.S. EPR Topical Report." The methodology to determine setpoints for all other RT and ESF functions is documented in Topical Report ANP-10275P.

In RAI 321, Question 07.01-20, the staff requested that the applicant clarify whether or not the single-sided distribution will be used in the U.S. EPR design certification application. If the single-sided distribution will be used, then the applicant is requested to provide detailed discussion which demonstrates how the U.S. EPR design certification application will meet the 95/95 criteria in RG 1.105 using the single-sided distribution. 10 CFR 50.36 states, in part, that where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting shall be chosen so that automatic protective action will correct the abnormal situation before a safety limit is exceeded. RG 1.105, "Setpoints for Safety Related Instrumentation," Revision 3, states, "The 95/95 tolerance limit is an acceptable criterion for uncertainties." Topical Report ANP-10275P was accepted by NRC and it stated that the U.S. EPR may utilize the one-sided distribution for setpoint calculation if the channel approaches a trip in only one direction. In order to obtain the desired 95 percent probability for one-sided normal distribution, the trip setpoints must be set 1.645 standard deviations from the design basis analytical limit. In RAI 321, Question 07.01-20 the staff also requested that the applicant state whether the one-sided distribution with a reduction factor would be used, and if it will be used, to provide the technical basis demonstrating how the use of the one-sided distribution with the 1.645 reduction factor meets the 95/95 criteria of RG 1.105. In a March 5, 2010 response to the RAI 321 Question 07.01-20, the applicant indicated that the single-sided distribution would not be used. The staff verified that the U.S. EPR design certification application was updated accordingly. Based on the staff's findings in the safety evaluation reports to Topical Report ANP-10275 and ANP-10287, the U.S. EPR design meets IEEE Std 603-1998, Clause 6.8.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be design with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including AOOs. In the US EPR design, steady state and transient analyses are

performed to assure that reactor coolant system design conditions are not exceeded during normal operation. Protection and control setpoints are based on these analyses. The I&C systems may contribute to reactor coolant system design margin in many ways, for example, by providing better than the minimum required performance, as conservatism in setpoint calculations, or by system features that make the protection or control systems more fault tolerant. The setpoints used for I&C safety systems are implemented according to an approved setpoint methodology. The NRC staff finds that the requirements of GDC 15 have been adequately addressed in I&C safety systems.

#### **7.1.4.26      *Three-Mile Island Action Plan Items***

The staff's evaluation on U.S. EPR compliance to the Three Mile Island Action Plan requirements as identified in 10 CFR 50.34(f) is discussed in Section 7.5.4.1 of this report.

### **7.1.5            Combined License Information Items**

No applicable items were identified in the FSAR. No additional combined license (COL) information items need to be included in FSAR Tier 2, Table 1.8 2, "U.S. EPR Combined License Information Items," for I&C Systems - Introduction.

### **7.1.6            Findings and Conclusions**

The staff review confirms that the applicant provided sufficient information to support the following conclusions. The applicant identified the I&C systems that are important to safety in accordance with RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)," and identified the NRC regulations that are applicable to these systems. The applicant has also identified appropriate guidelines consisting of the regulatory guides and the industry codes and standards that are applicable to the systems.

10 CFR 50.55a(a)(3) allows applicants under 10 CFR Part 52 to propose alternatives to the requirements of 10 CFR 50.55a(h) or portions thereof. 10 CFR 50.55a(h)(3) requires the use of IEEE Std 603-1991. The staff evaluated and accepted the applicant's proposed alternative to use IEEE Std 603-1998 in lieu of IEEE Std 603-1991. Upon satisfactory resolution of RAI 505, Question 07.01-33 in Section 7.1.4.1.2 of this report, the staff finds the applicant's proposed alternative to IEEE Std 603-1998, Clause 5.6.1 acceptable.

The staff reviewed the application against the requirements of IEEE Std 603-1998. The clauses within IEEE Std 603-1998 address, among other requirements, single failure protection, independence, quality, design bases, information displays, automatic and manual controls, operating and maintenance bypasses, and capability for test and calibration. Several open items were identified in the staff's review of IEEE Std 603-1998. Upon satisfactory resolution of the open items, the staff finds that the U.S. EPR design meets the requirements of IEEE Std 603-1998.

The staff reviewed the U.S. EPR design to verify its compliance with the following applicable regulatory requirements; 10 CFR 50.55a(a)(1), as it relates to quality standards for systems important to safety, and GDC 1. The staff finds that the applicant meets the requirements of 10 CFR 50.55a(a)(1) and GDC 1.

In conjunction of the staff's review of IEEE Std 603-1998, the staff reviewed compliance of the design to GDC 2, GDC 4, GDC 13, GDC 20, GDC 21, GDC 22, GDC 23, GDC 24, and

GDC 29. As noted with the review of IEEE Std 603-1998, several open items were identified, and upon their satisfactory resolution, the U.S. EPR design meets the requirements of GDC 2, GDC 4, GDC 13, GDC 20, GDC 21, GDC 22, GDC 23, GDC 24, and GDC 29.

The staff reviewed the ITAAC in regards to compliance to 10 CFR 52.47(b)(1). Additional discussion on the staff's review of compliance to 10 CFR 52.47(b)(1) is found in Section 14.3.5 of this report. As noted within Section 14.3.5 of this report and in this section, several open items were identified regarding the ITAAC, and upon their satisfactory resolution, the U.S. EPR design meets the requirements of 10 CFR 52.47(b)(1).

Once the identified open items and confirmatory items noted above are satisfactorily resolved, the staff should be able to arrive at a conclusion that the implementation of the identified acceptance criteria and guidelines in Section 7.1 of this report satisfies the above stated applicable requirements with respect to the design, fabrication, erection, and testing commensurate with the importance of the safety functions to be performed.

## **7.2 Reactor Trip System**

The U.S. EPR provides safety related I&C to sense conditions requiring protective action and automatically initiate an RT. Manual initiation of an RT at the division level is also available.

### **7.2.1 Introduction**

The PS initiates automatic RT to rapidly introduce negative reactivity to the core to mitigate the effects of AOOs and postulated accidents, and to prevent acceptable fuel design limits from being exceeded. The PS automatically initiates an RT when selected variables exceed setpoints that are indicative of conditions which require protective action. Additionally, the ability to manually initiate the RT function is provided in the MCR and the RSS. Initiation of the RT function results in removal of electrical power from the control rod drive mechanism (CRDM) coils, allowing the rods to fall by gravity into the core.

### **7.2.2 Summary of Application**

**FSAR Tier 1:** The FSAR Tier 1 information associated with this Section is found in FSAR Tier 1, Section 2.4, "Instrumentation and Control Systems." In FSAR Tier 1, Section 2.4.1, "Protection System," the applicant states that the protection system is provided to sense conditions requiring protective action and automatically initiate the safety systems required to mitigate the event. The PS provides the following safety related functions for the RT system:

- Performs automatic initiation of RT functions
- Provides for initiation of RT manual functions
- Generates permissive signals that authorize the activation or deactivation of certain protective actions according to current plant conditions
- Generates permissive signals that maintain safety-related interlocks

**FSAR Tier 2:** The applicant provided a system description in FSAR Tier 2, Section 7.2, "Reactor Trip System," summarized here, in part, as follows:

The PS processes both automatic and manual RT functions. Each RT function is performed redundantly and independently in each of the four PS divisions. A RT order, produced by any two of the four divisions, results in a reactor shutdown. In-core instrumentation, ex-core instrumentation, and process instrumentation are the three process variables that are continuously monitored to determine the safety status of the plant and are used as inputs to automatic RT functions. Any one of two different sets of RT devices can successfully remove power to the CRDM coils. The two sets are the RT breakers and the RT contactors. When an RT order is generated, the PS acts on both sets of RT devices.

**ITAAC:** The ITAAC associated with FSAR Tier 2, Section 7.2, are specified in FSAR Tier 1, Table 2.4.1-7 of the Revision 3 interim mark-ups, "Protection System ITAAC."

**Technical Specifications:** The Technical Specifications associated with FSAR Tier 2, Section 7.2 are specified in FSAR Tier 2, Chapter 16, "Technical Specifications," specifically, Section 3.3 of the Technical Specifications. Chapter 16 of this report provides the staff evaluation of the Technical Specifications related to the RT system.

### 7.2.3 Regulatory Basis

The relevant requirements of the NRC regulations for this area of review, and the associated acceptance criteria, are specified in NUREG-0800, Section 7.2, "Reactor Trip System," and are summarized below. Review interfaces with other SRP Sections also can be found in NUREG-0800, Section 7.2.

10 CFR Part 50, Appendix A, "General Design Criterion for Nuclear Power Plants:"

1. GDC 10, "Reactor Design" as it relates to the reactor core and associated coolant, control, and protection systems to assure that specified acceptable fuel design limits are not exceeded during any conditions.
2. GDC 15, "RCS (RCS) Design," to ensure the reactor coolant system and associated auxiliary, control, and protection systems design has sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition.
3. GDC 20, "Protection Systems Functions," as it relates to protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety
4. GDC 25, "Protection System Requirements for Reactivity Control Malfunctions," to ensure that the protection system design assures that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems.
5. 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet, January 30, 1995
6. 10 CFR 52.47(b)(1), "Contents of applications; technical information," requires that a design certification contain the proposed inspections, tests, analyses, and acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the

inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act of 1954, and NRC regulations.

Acceptance criteria adequate to meet the above requirements include:

SRP Table 7 1, "Regulatory Requirements (R), and SRP Acceptance Criteria (A) for Instrumentation and Control Systems Important to Safety," Section 3 (Staff Requirements Memoranda), Section 4 (Regulatory Guides), and Section 5 (Branch Technical Positions), lists the SRP acceptance criteria applicable to the reactor trip system.

#### **7.2.4 Technical Evaluation**

The objective of the staff's evaluation is to confirm that the reactor trip design satisfies NRC regulations through a set of acceptance criteria and that it can perform its safety functions for all plant conditions. SRP Section 7.2 lists regulatory acceptance criteria for design considerations that should be emphasized for the review of reactor trip functions. The acceptance criteria are covered by the reactor trip review under the headings listed in Table 7.3-1 below. Most of these design considerations are addressed in other Sections of this report, and where appropriate, the evaluation for Section 7.2 refers to other Sections for additional details. Table 7.2 1 below lists the Sections in this report where the specified design considerations are addressed.

**Table 7.2-1 Section 7.2 Design Considerations Referenced in Other Sections of this Report.**

<b>Design Consideration</b>	<b>SER Section(s)</b>
Quality Standards, 10 CFR 50.55a(a)(1) and GDC 1	7.1.4.3, 7.1.4.7
Design Bases, 10 CFR 50.55a(h), GDC 16, GDC34, GDC 35, GDC 38, GDC 41 and GDC 44	7.3
Quality Standards, - 10 CFR 50.55a(a)(1) and GDC 1	7.1.4.3, 7.1.4.7
Design Bases - 10 CFR 50.55a(h) and GDC 16, GDC 28, GDC 33, GDC 34, GDC 35, GDC 38, GDC 41, and GDC 44	7.3.4
Single Failure Protection, 10 CFR 50.55a(h) and GDC 21	7.1.4.5
Completion of Protective Action – 10 CFR 50.55a(h)	7.1.4.6
Quality – 10 CFR 50.55a(h) and GDC 1	7.1.4.7
Independence, 10 CFR 50.55a(h), GDC 21, GDC 22 and GDC 24	7.1.4.10, 7.9.4
Equipment Qualification, 10 CFR 50.55a(h) GDC 2 and, GDC 4	7.1.4.8, 3.10, 3.11
System Integrity, 10 CFR 50.55a(h)	7.1.4.9

Design Consideration	SER Section(s)
Capability for Test and Calibration, 10 CFR 50.55a(h), and GDC 21	7.1.4.11
Information Displays, 10 CFR 50.55a(h), GDC 13, and GDC 19	7.1.4.12, 7.5.4,
Control of Access, 10 CFR 50.55a(h)	7.1.4.13, 7.9.4.3
Repair, 10 CFR 50.55a(h)	7.1.4.14
Identification, 10 CFR 50.55a(h)	7.1.4.15
Auxiliary Features, 10 CFR 50.55a(h)	7.1.4.16
Multi-Unit Stations, 10 CFR 50.55a(h)	7.1.4.17
Human Factors Considerations, 10 CFR 50.55a(h) and GDC 19	7.1.4.19, 18.0
Reliability, 10 CFR 50.55a(h) and GDC 21	7.1.4.20
Automatic and Manual Control, 10 CFR 50.55a(h)	7.1.4.22
Derivation of System Inputs, 10 CFR 50.55a(h)	7.1.4.18
Bypasses (Operating and Maintenance), 10 CFR 50.55a(h), GDC 13 and GDC 19	7.1.4.23, 7.1.4.24, 7.5.4.2
Setpoints, 10 CFR 50.55a(h)	7.1.4.25
TMI-Related Requirements, 10 CFR 50.34(f)	7.5.4.1
Diversity and Defense-in-Depth, 10 CFR 50.55a(h), and GDC 22	7.1.4.21, 7.8
Inspections, Tests, Analyses, and Acceptance Criteria, 10 CFR 52.47(b)(1)	14.3.5

10 CFR 50.55a(a)(3) allows an applicant under 10 CFR Part 52 to propose alternatives to the requirements of 10 CFR 50.55a(h). The U.S. EPR design certification applicant proposes to use IEEE Std 603-1998, as an alternative to 10 CFR 50.55a(h), which requires the use of IEEE Std 603-1991. Section 7.1.4.1.1 of this report discusses the staff's evaluation and approval of this alternative.

The staff's evaluation on the reactor trip system presented in this section is based on IEEE Std 603-1998 and the scope of the evaluation is limited to Section 4, "Design Bases," in IEEE Std 603-1998 and the applicable GDC.

The staff's review of the I&C systems conducted in this section is based on the docketed FSAR, Revision 2. However, since FSAR Revision 2, was submitted, the applicant made several changes to the I&C system design as part of request for additional information (RAI) responses. Those new design changes were not a result of the specific response to RAI that transmitted them to the staff, but were incorporated in the mark-ups for FSAR Tier 1, Section 2.4 and FSAR Tier 2, Chapter 7, Interim Revision 3 mark-ups. Specifically, the **June 22, 2011, response to RAI 452, Question 07.03-36, and the May 25, 2011, response to RAI 442,**

**Question 07.01-27, which provide the FSAR Tier 1 and 2, Interim Revision 3 mark-ups, will be tracked as a confirmatory items.**

#### 7.2.4.1 *System Description*

Technical Report ANP-10309P, "U.S. EPR Protection System Technical Report," Revision 3, Section 1.0 states that the PS, is implemented using TELEPERM XS technology, and it is both digital, integrated reactor protection system and an ESF actuation system.

FSAR Tier 2, Section 7.2.1, "Description," describes the purpose of the PS, which is to mitigate the effects of anticipated operational occurrences and postulated accidents, and to prevent acceptable fuel design limits from being exceeded. When selected variables exceed setpoints, the PS automatically initiates a reactor trip to rapidly introduce negative reactivity to the core. RT can also be manually initiated through the SICS in the MCR and the RSS. When the reactor trips, electrical power is removed from the coils of the control rod drive mechanism. With no power to engage the control rods, the rods fall by gravity into the core, and introduce negative reactivity.

FSAR Tier 2, Section 7.2.1.1, "System Description," describes the RT system. The PS handles both automatic and manual reactor trip functions, and each function is performed redundantly and independently in each of the four PS divisions. To determine the safety status of the plant, three categories of variables are monitored: in-core instrumentation, ex-core instrumentation, and process instrumentation. In-core instrumentation uses SPND inputs to calculate variables that cannot be directly measured such as linear power density and departure from nucleate boiling ratio. Ex-core instrumentation uses power range detectors and intermediate range detectors to provide measurements of reactor power, and these detectors are used to provide inputs to RT functions that detect conditions such as high neutron flux and low doubling time. Process instrumentation is used to measure variables such as pressure, temperature, and flow, and these process measurements are used to initiate RT or as inputs to calculations of variables that cannot be measured directly. When an RT order, produced by any two of the four divisions, is generated, the PS acts on the two sets of different devices that can remove electrical power from the CRDM coils: RT breakers and RT contactors. FSAR Tier 2, Section 7.2.1.1, describes the sequence performed by the PS to initiate an automatic RT. RT actuation sequence is illustrated in FSAR Tier 2, Figure 7.2 1, "Typical RT Actuation." An APU in each of the four PS divisions acquires one-fourth of the redundant sensor measurements that serve as inputs to a specified RT function from the SCDS. However, for the SPND measurements, each PS division acquires each of the 72 SPND signals as stated in Section 7.1 of Technical Report ANP-10309P. The APU performs required processing or calculations, and compares the resulting variable to a relevant setpoint. If the setpoint is exceeded, a partial trigger signal is generated. The partial trigger signals are sent to redundant ALUs in all four divisions where two out of four logic is performed. If partial trigger signals are present in at least two of the four divisions, the ALU in all four divisions generates RT signals. The RT signals of the redundant ALU in each subsystem are combined in a hardwired "functional AND gate" logic, and if an RT signal is present in both ALUs, an RT output is generated. The RT outputs from both subsystems in a division are combined in a hardwired functional OR gate logic, and if either subsystem produces an RT output, a divisional RT order is generated. The divisional RT order then propagates to two sets of devices that remove electrical power from the coils of the CRDM; RT breakers, and contactors.

Technical Report ANP-10309NP, Chapter 5 further describes the APU and ALU. Each PS division has three APUs assigned to Subsystem A, and two APUs are assigned to

Subsystem B. Each APU of a division is redundant to the corresponding APU of the other three PS divisions. The APU primary functions are to acquire the signals from the process sensors and monitoring systems via the SCDS, to perform processing (e.g., calculations and setpoint comparisons) using the input signals, and to distribute the results to the ALU for voting. Each PS division has four ALUs, two assigned to each subsystem. The two ALUs in each subsystem are redundant, and to avoid spurious RT actuations, their outputs are combined in a hardwired “functional AND” logic for RT outputs. The actuation orders from the ALU are sent to the trip devices for RT actuations. The ALU primary functions are to perform voting of processing results from the redundant APU in the various divisions and to issue actuation orders based on the voting results. The ALU also contains the logic used to latch and either manually, or automatically, unlatch actuation outputs. Section 7.2.4.2.3 of this report discusses ALU and manual actuation. Technical Report ANP-10309P, Chapter 7 describes the characteristics of the trip breakers and trip contactors of the CRDM operating coils. Each PS division is assigned to one of four trip breakers; each divisional RT order acts on the under voltage coil of the assigned breaker (de-energize to open). PS Divisions 1 and 2 open trip breakers are located in Division 2 Safeguard Building. PS Divisions 3 and 4 open trip breakers are located in Division 3 Safeguard Building. The trip breakers are arranged in a “1 out of 2 taken twice” configuration and requires the following logical combination of PS divisional RT orders to actuate an RT: (1 or 2) and (3 or 4). There are 23 sets of four trip contactors. Each set of four contactors can remove power to four CRDM power supplies and is arranged in a 2 out of 4 configuration. Eleven sets of contactors are in Division 1, and 12 sets are in Division 4. Each division is assigned to one contactor in each of the 23 sets.

#### 7.2.4.2 *Design Basis Events*

The staff used the guidance found in NUREG-0800, Revision 5, Appendix 7.1 C, “Guidance for Evaluation of Conformance to IEEE Std 603,” to evaluate the application against the regulations. IEEE Std 603-1998, Section 4 lists the design basis requirements for reactor trip functions.

##### 7.2.4.2.1 *Design Basis Events, Protective Actions, and Monitored Variables*

IEEE Std 603-1998, Clause 4.a requires the identification of the design basis events applicable to each mode of operation along with the initial conditions and allowable limits of plant conditions for each such event. IEEE Std 603-1998, Clause 4.b also requires the safety functions and corresponding protective actions of the execute features for each design basis event be identified. Additionally, 10 CFR Part 50, Appendix A, GDC 10, requires the reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. GDC 20 requires the PS to automatically initiate the reactivity control systems and to sense accident conditions and initiate the operation of systems and components important to safety. GDC 25 requires the protection system be designed to assure that fuel limits are not exceeded for a single failure of the reactivity control system such as an accidental rod withdrawal. SRP Appendix 7.1-C identifies SRP BTP 7-5, “Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors,” to contain acceptance criteria for meeting these two requirements. SRP BTP 7-5 recommends that operator error be considered along with a single failure of the reactivity control systems when evaluating GDC 20 and GDC 25.

FSAR Tier 2, Section 7.2.2.1.1, “Design Basis: Applicable Events (Clause 4.a and 4.b of IEEE Std 603-1998),” states that design basis events requiring protective action with initial



conditions are analyzed in FSAR Tier 2, Chapter 15, "Transient and Accident Analyses." FSAR Tier 2, Table 15.0-1, "U.S. EPR Initiating Events," lists the initiating events analyzed. FSAR Tier 2, Table 15.0-10, "Plant Systems Used in the Accident Analysis," lists initiating events which lead to a protective action and the corresponding RT function. The staff review of the design basis events and the corresponding reactor trip functions is discussed in Chapter 15 of this report. FSAR Tier 1, Table 2.4.1-7, Item 4.1 provides an ITAAC to verify these design requirements.

FSAR Tier 2, Table 7.2-1, "Reactor Trip Variables," lists the protective functions, variables to be monitored, and the ranges of the variable. This FSAR table is duplicated below.

**Table 7.2-2 Reactor Trip Functions**

[Source: FSAR Tier 2, Table 7.2-1, Revision 2]

Protective Function	Variables To Be Monitored	Range of Variables
High Linear Power Density	Neutron Flux-Self Powered Neutron Detectors	0 - 590 W/cm
Low Departure From Nucleate Boiling Ratio (DNBR)	Neutron Flux-Self Powered Neutron Detectors	0 - 590 W/cm
	Cold Leg Temperature Narrow Range(NR)	500 °F - 626 °F
	RCP Speed	800 - 1,600 rpm
	RCS Loop Flow	0-120% Nominal Flow (NF)
	RCCA position	0 – 100% Insertion
	Pressurizer Pressure (NR)	1,615 – 2,515 psia
High Neutron Flux Rate of Change	Neutron Flux-Power Range Detectors (PRD)	0.5 - 200% Nuclear Power (NP)
High Core Power Level	Cold Leg Temperature Wide Range (WR)	32 °F – 662 °F
	Hot Leg Pressure (WR)	15 – 3,015 psia
	Hot Leg Temperature (NR)	536 °F - 662 °F
	RCS Loop Flow	0-120% NF
Low Reactor Coolant Pump (RCP) Speed	RCP Speed	800 - 1,600 rpm
Low RCS Flow Rate (two loops)	RCS Loop Flow	0 – 120% NF
Low-Low RCS Flow Rate (one loop)	RCS Loop Flow	0 – 120% NF
Low Doubling Time	Neutron Flux-Intermediate Range Detector	5 x 10E-6 - 60% NP
High Neutron Flux	Neutron Flux-Intermediate	5 x 10E-6 - 60% NP

Protective Function	Variables To Be Monitored	Range of Variables
	Range Detector	
Low Pressurizer Pressure	Pressurizer Pressure (NR)	1,615 – 2,515 psia
High Pressurizer Pressure	Pressurizer Pressure (NR)	1,615 – 2,515 psia
High Pressurizer Level	Pressurizer Level (NR)	0-100% Measuring Range (MR)
Low Hot Leg Pressure	Hot Leg Pressure (WR)	15 – 3,015 psia
SG Pressure Drop	SG Pressure	15 – 1,615 psia
Low SG Pressure	SG Pressure	15 – 1,615 psia
High SG Pressure	SG Pressure	15 – 1,615 psia
Low SG Level	SG Level (NR)	0 – 100% MR
High SG Level	SG Level (NR)	0 – 100% MR
High Containment Pressure	Containment Service Compartment Pressure (NR)	-3 psig to + 7 psig
	Containment Equipment Compartment Pressure	-3 psig to + 7 psig
Low Saturation Margin	Cold Leg Temperature (WR)	32°F - 662°F
	Hot Leg Pressure (WR)	15 – 3,015 psia
	Hot Leg Temperature (NR)	536 °F – 662 °F
	RCS Loop Flow	0-120% NF

In addition to the plant or process conditions that cause RT, these safety-related signals also initiate RT: safety injection system actuation, EFW system actuation, and manual RT signals from SICS.

FSAR Tier 2, Section 7.2.1, identifies the PS as the system that will automatically initiate a reactor trip when selected variables exceed their setpoint. Safety-related instrumentation senses these plant process variables and provides input to the PS for determining the need for an RT. Single failure protection of the PS is discussed in Section 7.1.4.5 of this report. Evaluation of single failures such as accidental rod withdrawals, whether based on the reactivity control system or operator error, is discussed in Chapter 15 of this report.

Based on the information described above, the staff finds that the RT system meets IEEE Std 603-1998, Clauses 4.a and 4.b, since the applicant identified design basis events and the corresponding protective actions for each of those events through the accident analysis in FSAR Tier 2, Chapter 15.

IEEE Std 603-1998, Clause 4.d requires, in part, the identification of variables that are monitored in order to provide protective action. IEEE Std 603-1998, Clause 4.d also requires the identification of the analytical limit associated with each variable and the ranges. FSAR Tier 2, Table 7.2-1 identifies variables to be monitored and their ranges. FSAR Tier 2, Table 15.0-7, “Reactor Trip Setpoints and Delays Used in the Accident Analysis,” identifies the analytical limits for reactor trip function signals.

IEEE Std 603-1998, Clause 4.d requires, in part, the identification of the rates of change of these variables to be accommodated until proper completion of protective action is ensured. In RAI 413, Question 07.02-32, the staff requested that the applicant address IEEE Std 603-1998, Clause 4.d with regards to the identification of the rates of change of variables to be accommodated until proper completion of protective action is ensured. In a March 23, 2011 response to RAI 413, Question 07.02-32, the applicant committed to updating FSAR Tier 2, Section 7.1.2.6.3, with additional supporting statements such as sensor response time and PS cycle times required to accommodate the rates of change of monitored variable. The applicant added supporting statements to FSAR Tier 2, Section 7.1.2.6.3, Interim Revision 3 mark-ups. FSAR Tier 1, Table 2.4.1 7, Item 4.7, provides an ITAAC to verify these design requirements. Since the applicant identified the variables that are monitored in order to provide protective action and the associated analytical limits and the rate of change of variables to be accommodated until proper completion of protective action is ensured, the staff finds that the reactor trip system meets IEEE Std 603-1998, Clause 4.d.

#### 7.2.4.2.2 *Permissives*

IEEE Std 603 1998, Clause 4.c requires the identification of the permissive conditions for each operating bypass capability that is to be provided.

FSAR Tier 2, Section 7.2.1.3, "Permissive Signal Functional Description," identifies the permissive conditions or operating bypasses for each RT functions identified. Permissive signals are used to enable, disable, or modify the operation of RT ESF actuation functions based on plant conditions. Permissive signals carry either a logical value of zero for an inhibited state or one for a validated state. P AUTO is a permissive that is automatically validated or inhibited based on the corresponding plant condition. P MANU is a permissive that is manually validated or inhibited by operator action after the corresponding plant condition has been satisfied. The operator activates permissives through the SICS. Thirteen permissives are identified in FSAR Tier 2, Section 7.2.1.3, and they are duplicated in the following table for information purposes.

**Table 7.2-3 Permissives**

[Source: FSAR Tier 2, Section 7.2.1.3, Revision 2]

Permissive	Validation	Inhibition	Description
P2	P-AUTO	P-AUTO	Permissive is representative of PRD neutron flux measurements higher than a low-power setpoint value (10% power). The P2 setpoint value corresponds to the value below which transients do not lead to risk of departure from nucleate boiling (DNB).
P3	P-AUTO	P-AUTO	Permissive is representative of PRD neutron flux measurements higher than an intermediate power setpoint value (70% power). The P3 setpoint value corresponds to value below which loss of one reactor coolant pump does not lead to risk of DNB.
P5	P-AUTO	P-AUTO	Permissive is representative of IRD neutron flux measurements above a low-power

Permissive	Validation	Inhibition	Description
			setpoint value (10-5 % power). The P5 setpoint value corresponds to boundary between the operating ranges of the source range detectors and intermediate range detectors.
P6	P-MANU	P-AUTO	Permissive is representative of core thermal power above a low-power setpoint value (10% power) corresponding to the boundary between the operating ranges of the IRDs and the PRDs.
P7	P-AUTO	P-AUTO	Permissive defines when reactor coolant pumps are no longer in operation.
P8	P-AUTO	P-AUTO	Permissive defines the shutdown state with all rods in (ARI).
P12	P-MANU	P-AUTO	Permissive facilitates plant heatup and cooldown by disabling certain ESF functions.
P13	P-MANU	P-AUTO	Permissive defines when SG draining and filling operations are allowed.
P14	P-MANU	P-MANU	Permissive defines when the residual heat removal (RHR) system is allowed to be connected to the RCS.
P15	P-MANU	P-AUTO	Permissive defines when safety injection (SI) actuation due to $\Delta P_{sat}$ is disabled and SI actuation due to low loop level is enabled.
P16	P-MANU	P-MANU, concurrent with reactor trip reset or hot leg pressure > 289.7 psia	Permissive defines when the SIS may be aligned from cold leg injection to hot leg injection.
P17	P-MANU	P-AUTO	Permissive corresponds to the temperature conditions where brittle fracture protection is required.
P18	P-AUTO	P-AUTO	Permissive prevents the unsafe positioning of the SG transfer valves

FSAR Tier 1, Table 2.4.1 7, Item 4.3, provides an ITAAC to verify these design requirements. Since the applicant has identified the permissive conditions and sufficient ITAAC have been provided, the staff finds that the reactor trip system meets IEEE Std 603 1998, Clause 4.c.

#### *7.2.4.2.3 Protective Actions Using Manual Means*

IEEE Std 603-1998, Clause 4.e describes the minimum criteria under which manual initiation and control of protective actions may be allowed. FSAR Tier 2, Section 7.2.2.1.4, "Design Basis: Manual Reactor Trip Initiation (Clause 4.e of IEEE Std 603-1998)," states that there are no operating bypasses placed on the manual RT function, it is available at any time, under any plant conditions. IEEE Std 603 1998, Clause 4.e requires the variables in 4.d to be displayed for the operator to use in taking manual actions. FSAR Tier 2, Section 7.2.2.1.4, states that the variables to be displayed to the operator to use in manual RT initiation are determined as part of the methodology used for selecting Type A variables as described in FSAR Tier 2, Section 7.5, "Information Systems Important to Safety." FSAR Tier 2, Table 7.5-1, identifies the PAM variables and their types, including Type A variables. FSAR Tier 1, Table 2.4.1 7, Item 4.11 and other PAM ITAACs described in Sections 7.5 and 14.3.5 of this report provide a verification of this design requirement. Since the applicant identified the criteria under which manual initiation and control of protective actions may be performed, the staff finds that the reactor trip system meets IEEE Std 603-1998, Clauses 4.e.1, 4.e.2, and 4.e.3.

#### *7.2.4.2.4 Spatially Dependent Variables*

IEEE Std 603-1998, Clause 4.f requires, in part, the identification of the minimum number and location of sensors for those variables in IEEE Std 603-1998, Clause 4.d that have a spatial dependence. The applicant's analysis should demonstrate that the number and location of sensors are adequate.

FSAR Tier 2, Section 7.2.2.1.5, "Design Basis: Spatially Dependent Variables (Clause 4.f of IEEE Std 603-1998)" states the SPNDs are located systematically throughout the core to provide spatially dependent neutron flux information. FSAR Tier 2, Section 4.4.6.1, "Fixed In-core Instrumentation," states SPNDs are distributed at 12 radial core locations with six detectors distributed axially in each radial location. FSAR Tier 2, Figure 4.4 8, "Arrangement of In-core Instrumentation (Top View)," provides the top view of in-core instrumentation arrangement. A similar figure is Topical Report ANP 10287P, "Topical Report of In core Trip Setpoint and Transient Methodology for U.S. EPR," Revision 0, Figure E 1, as the HLPD and low DNBR reactor trip functions take these spatial variations into account. The RT logic can accommodate any five failed SPNDs for HLPD function, and any number of failed SPND on up to five fingers for the low DNBR function. U.S. EPR Technical Specifications, Table 3.3.1 1, "Protection System Sensors, Manual Actuation Switches, Signal Processors, and Actuation Devices," shows that 67 of 72 SPNDs are the minimum required.

FSAR Tier 2, Section 7.2.2.1.5, also identifies four spatially dependent temperature sensors in each hot leg, with each sensor mounted approximately 90 degrees apart in a cross sectional plane of the piping. The four measurements are averaged to obtain a value of hot leg temperature. PS can accommodate up to two failed sensors in each hot leg.

FSAR Tier 1, Table 2.4.1 7, Item 4.7, provides an ITAAC to verify the design commitments for spatially-dependent sensors. Based on the discussion above, the applicant identified the spatially-dependent sensors and their location so the reactor trip system meets IEEE Std 603-1998, Clause 4.f.

#### 7.2.4.2.5 *Critical Points in Time or Plant Conditions*

IEEE Std 603 1998, Clause 4.j requires identification of the critical points in time or plant conditions after the onset of design basis event including:

- (4.j.1) the point in time or plant conditions for which the protective actions of the safety system shall be initiated
- (4.j.2) the point in time or plant conditions that define the proper completion of the safety function
- (4.j.3) the point in time or the plant conditions that require automatic control of protective actions
- (4.j.4) the point in time or the plant conditions that allow returning a safety system to normal

FSAR Tier 2, Section 7.2.2.1.6, "Design Basis: Critical Points in Time or Plant Conditions (Clause 4.j of IEEE Std 603 1998)," states that RT is initiated by the PS when selected variables exceed the associated RT setpoints. The plant conditions that define the proper completion of the RT function are defined on an event by event basis in the FSAR Tier 2, Revision 2, Chapter 15 analyses. The section also states the RT function only resets (returned to normal) after manual actions have been taken to close the RT breakers, and that plant specific operating procedures govern the point in time when the RT breakers can be reset following an RT. FSAR Tier 2, Table 15.0 7, lists the reactor trip signal, its corresponding nominal setpoint and uncertainty, and the time delay. Time delay includes sensor delay, I&C delay, and the delay for the trip breakers to open and the stationary gripper to release. FSAR Tier 2, Table 15.0 10, lists the plant conditions and the corresponding protection system components to mitigate the design basis accident. The allowable conditions for returning a plant to normal operation are described in FSAR Tier 2, Chapter 16.

FSAR Tier 1, Table 2.4.1-2, "Protection System Automatic Reactor Trips," identifies the plant conditions for which the protective actions of the safety system shall be initiated. FSAR Tier 1, Table 2.4.1-7, Item 4.1, provides an ITAAC to verify the design commitments for critical points in time or plant conditions. Based on the discussion above, the reactor trip system meets IEEE Std 603-1998, Clause 4.j, for the identification of the point in time or plant conditions for which the protective actions of the safety system shall be initiated.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be design with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including AOOs. In the US EPR design, steady state and transient analyses are performed to assure that reactor coolant system design conditions are not exceeded during normal operation. Protection and control setpoints are based on these analyses. The I&C systems may contribute to reactor coolant system design margin in many ways, for example, by providing better than the minimum required performance, as conservatism in setpoint calculations, or by system features that make the protection or control systems more fault tolerant. The setpoints used for I&C protection system are implemented according to an approved setpoint methodology. The NRC staff finds that the requirements of GDC 15 have been adequately addressed in I&C systems.

## **7.2.5 Combined License Information Items**

No applicable items were identified in the FSAR. No additional COL information items need to be included in the FSAR Tier 2, Table 1.8 2, "U.S. EPR Combined License Information Items," for reactor trip system consideration.

## **7.2.6 Conclusions**

The staff reviewed the U.S. EPR reactor trip systems to verify their compliance to applicable regulations. Pending the confirmatory update to the FSAR, the staff concludes that the design of the RT system and the RT system initiation of auxiliary supporting features is acceptable and meet the relevant requirements of 10 CFR 50.55a(h), and 10 CFR Part 50, Appendix A, GDC 10, GDC 20,,and GDC 25.

The staff concludes that the RT system conforms to the design bases requirements of IEEE Std 603-1998, and therefore meets 10 CFR 50.55(a)(h). The RT system conforms to the guidance of RG 1.105, "Setpoints for Safety-Related Instrumentation." Based upon this review and coordination with those having primary review responsibility for the accident analysis, the staff concludes that the RT system includes the provision to sense accident conditions and AOO in order to initiate reactor shutdown in conformance with the accident analysis presented in FSAR Tier 2, Chapter 15, Revision 2, and evaluated by the staff in Chapter 15 of this report. Therefore, the staff finds that the RT system satisfies the requirements of GDC 10, GDC 15, and GDC 20.

Based on the review of the RT system, the staff concludes that the system satisfies the protection system requirements for malfunctions of the reactivity control system such as accidental withdrawal of control rods. FSAR Tier 2, Chapter 15 of this report address the capability of the system to ensure that fuel design limits are not exceeded for such events. Therefore, the staff finds that the RT system satisfies the requirements of GDC 25. The staff reviewed the ITAAC in regards to compliance to 10 CFR 52.47(b)(1). Additional discussion on the staff's review of compliance to 10 CFR 52.47(b)(1) is found in Section 14.3.5 of this report. As noted within Section 14.3.5 of this report, several open items were identified regarding the ITAAC, and upon their satisfactory resolution, the staff concludes that the U.S. EPR design meets the requirements of 10 CFR 52.47(b)(1).

## **7.3 Engineered Safety Features Systems**

### **7.3.1 Introduction**

The U.S. EPR provides safety-related instrumentation and controls to sense accident conditions and automatically initiate the ESF systems. ESF systems are automatically actuated when selected variables exceed setpoints that are indicative of conditions that require protective action. Additionally, the ability to manually initiate ESF systems is provided in the MCR. Manual system-level actuation of ESF systems initiates all actions performed by the corresponding automatic actuation, including starting auxiliary or supporting systems and performing required sequencing functions. Component-level control of ESF system actuators is also provided in the MCR.

### 7.3.2 Summary of Application

**FSAR Tier 1:** The FSAR Tier 1 information associated with this section is discussed in FSAR Tier 1, Section 2.4.1, for PS and Section 2.4.4 for the SAS. In FSAR Tier 1, Section 2.4.1, the applicant states that the PS is provided to sense conditions requiring protective action and automatically initiate the safety systems required to mitigate the event. The PS provides the following safety-related functions for the ESF:

- Performs automatic initiation of ESF functions
- Provides for actuation of ESF manual functions
- Generates permissive signals that authorize the activation or deactivation of certain protective actions according to current plant conditions
- Generates permissive signals that maintain safety-related interlocks

In FSAR Tier 1, Section 2.4.4, the SAS provides the following safety-related functions:

- Provides control and monitoring of systems required to transfer the plant to cold shutdown and maintain it in this state following an AOO or PA
- Provides control and monitoring of safety-related functions of auxiliary support systems
- Provides acquisition and processing of Type A, B, and C post-accident monitoring variables for display to the operators in the MCR and on the RSS
- Provides a safety interlock function

**FSAR Tier 2:** The applicant provided a system description in FSAR Tier 2, Section 7.3, "Engineered Safety Features Systems," summarized here, in part.

Automatic actuation of ESF systems and auxiliary supporting systems is performed by the PS when selected plant parameters reach the appropriate setpoints. These automatic actuation orders are sent to the PACS for prioritization and interface to the actuators. The ESF actuation sequence performed by the protection system is illustrated in FSAR Tier 2, Figure 7.3 1, and is described as follows:

- An APU in each division acquires one fourth of the redundant sensor measurements through the SCDS that are inputs to a given ESF actuation function.
- The APU in each division performs any required processing using the measurements acquired by that division (e.g., filtering, range conversion, calculations). The resulting variable is compared to a relevant actuation setpoint in each division. If a setpoint is exceeded, the APU in that division generates a partial trigger signal for the appropriate ESF function.
- The partial trigger signals from each division are sent to redundant ALU in the PS division responsible for the associated actuation. Two-out-of-four voting logic is performed in each ALU on the partial trigger signals from all four divisions. If the voting logic is satisfied, an actuation order is generated.



- The actuation signals of the redundant ALU in each subsystem are combined in hardwired “OR” configuration so that either redundant unit can actuate the function.

Actuation orders are sent from the PS to the PACS module associated with each actuator required for the function. The exception to this is the turbine trip function. The PS and the PACS are discussed in FSAR Tier 2, Section 7.1. The turbine control system is described in FSAR Tier 2, Section 10.2.

The SAS performs closed loop automatic controls of certain ESF systems following their actuation by the PS. These controls are described in FSAR Tier 2, Section 7.3.1.2, with their associated actuation functions. The SAS is described in FSAR Tier 2, Section 7.1.

The capability for manual system level ESF actuations is available to the operator through the SICS in the MCR. These manual actuations are acquired by the ALUs in the PS and combined with the automatic actuation logic. The manual actuations are described with the corresponding automatic function in FSAR Tier 2, Section 7.3.1.2.

The capability for component-level control of ESF system actuators is available to the operator on both the PICS and the SICS in the MCR. Commands from the PICS are processed by the PAS and sent to the PACS for prioritization. Commands from the SICS are sent directly to the PACS for prioritizations. The SICS is the safety-related actuation path and PICS is the non-safety-related actuation path. The manual system-level ESF actuation sequence is shown in FSAR Tier 2, Figure 7.3-1 (Sheet 2 of 5). The manual actuations are described with the corresponding automatic function in FSAR Tier 2, Revision 2, Section 7.3.1.2.

For an extra borating system malfunction event, the component-level controls on SICS are credited to terminate the event. For the failure of small lines carrying primary coolant outside the Reactor Building (see FSAR Tier 2, Section 15.0.3.5), component-level manual controls from SICS are credited to isolate the failed line. Operator actions credited in mitigating accidents are addressed in FSAR Tier 2, Section 15.0.0.3.7.

The capability for manual reset of sense and command ESF actuation outputs is provided on the SICS. Not all ESF actuations require a manual reset. There are cases where a sense and command output is cleared after the PS determines that the initiating condition has cleared. The reset functionality related to each ESF actuation is described in FSAR Tier 2, Section 7.3.1.2. Further description of the operation of the PICS and SICS is presented in FSAR Tier 2, Section 7.1.

**ITAAC:** The ITAAC associated with FSAR Tier 2, Section 7.3, are given in FSAR Tier 1, Table 2.4.1 7, and Table 2.4.4-6. The evaluation of ITAAC for this section will focus on the design bases requirements only.

**Technical Specifications:** The Technical Specifications associated with FSAR Tier 2, Section 7.3, is given in FSAR Tier 2, Chapter 16 (specifically Section 3.3, and B3.3 of the Technical Specifications and Technical Specifications bases), and its evaluation is addressed in Chapter 16 of this report.

### 7.3.3 Regulatory Basis

The relevant requirements of NRC regulations for this area of review, and the associated acceptance criteria, are given in Section 7.3, “Engineered Safety Features Systems,” of

NUREG-0800, Revision 5, and are summarized below. Review interfaces with other SRP Sections also can be found in NUREG-0800, Section 7.3.

1. GDC 10, "Reactor Design," as it relates to the reactor core and associated coolant, control, and protection systems to assure that specified acceptable fuel design limits are not exceeded during any conditions.
2. GDC 15 "Reactor Coolant System (RCS) Design," as it relates to controls providing sufficient margin to ensure the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.
3. GDC 16 "Containment design," as it relates to establishing an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and assuring that the containment design conditions important to safety are not exceeded
4. GDC 20, "Protection Systems Functions" as it relates to protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety
5. GDC 33, "Reactor Coolant Makeup," as it relates assuring a system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary.
6. GDC 34, "Residual Heat Removal," as it relates to assuring a system to remove residual heat is provided.
7. GDC 35, "Emergency Core Cooling," A system to provide abundant emergency core cooling shall be provided
8. GDC 38, "Containment Heat Removal ,"as it relates to assuring a system to provide abundant emergency core cooling is provided
9. GDC 41, "Containment Atmosphere Cleanup," as it relates to assuring Systems to control fission products, hydrogen, oxygen, and other substances which may be released into the reactor containment are provided
10. GDC 44, "Cooling Water," as it relates to assuring that a system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink is provided.
7. 10 CFR 52.47(b)(1), "Contents of applications; technical information," requires that a design certification contain the proposed inspections, tests, analyses, and acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act of 1954, and NRC regulations.
11. 10 CFR 52.80(a), "Contents of Applications; Additional Technical Information."

12. 10 CFR 50.55a(h), "Protection and Safety Systems."

Acceptance criteria adequate to meet the above requirements include SRP Table 7 1, Section 3 (Staff Requirements Memoranda), Section 4 (Regulatory Guides), and Section 5 (Branch Technical Positions), which lists the SRP acceptance criteria applicable to ESF systems.

### 7.3.4 Technical Evaluation

The objective of the staff's evaluation is to confirm that the ESF design satisfies NRC regulations through a set of acceptance criteria and that it can perform its safety functions for all plant conditions. SRP Section 7.3 lists regulatory acceptance criteria for design considerations that should be emphasized for the review of ESF. The acceptance criteria are covered by the ESF review under the headings listed in Table 7.3-1 below. Most of these design considerations are addressed in other sections of this report, and where appropriate, the evaluation for FSAR Tier 2, Section 7.3 refers to other sections for additional details. Table 7.3-1 below lists the sections in this report where the specified design considerations are addressed.

**Table 7.3-1 Section 7.3 Design Considerations Referenced in Other Sections of this Report..**

<b>Design Consideration</b>	<b>SER Section(s)</b>
Quality Standards, 10 CFR 50.55a(a)(1) and GDC 1	7.1.4.3, 7.1.4.7
Single Failure Protection, 10 CFR 50.55a(h), GDC 21	7.1.4.5
Completion of Protective Action – 10 CFR 50.55a(h)	7.1.4.6
Quality – 10 CFR 50.55a(h), GDC 1	7.1.4.7
Independence, 10 CFR 50.55a(h), GDC 21, GDC22, and GDC 24	7.1.4.10, 7.9.4
Equipment Qualification, 10 CFR 50.55a(h), GDC 2, and GDC44	7.1.4.8, 3.10, 3.11
System Integrity, 10 CFR 50.55a(h)	7.1.4.9
Capability for Test and Calibration - 10 CFR 50.55a(h) and GDC 21	7.1.4.11
Information Displays - 10 CFR 50.55a(h), GDC 13, and GDC 19	7.1.4.12, 7.5.4
Control of Access - 10 CFR 50.55a(h)	7.1.4.13, 7.9.4.3
Repair - 10 CFR 50.55a(h)	7.1.4.14
Identification - 10 CFR 50.55a(h)	7.1.4.15
Auxiliary Features - 10 CFR 50.55a(h)	7.1.4.16
Multi-Unit Stations - 10 CFR 50.55a(h)	7.1.4.17
Human Factors Considerations, 10 CFR 50.55a(h) and GDC 19	7.1.4.19, 18.0
Reliability - 10 CFR 50.55a(h) and GDC 21	7.1.4.20

Design Consideration	SER Section(s)
Automatic and Manual Control - 10 CFR 50.55a(h)	7.1.4.22
Derivation of System Inputs - 10 CFR 50.55a(h)	7.1.4.18
Bypasses (Operating and Maintenance), 10 CFR 50.55a(h), GDC 13 and GDC 19	7.1.4.23, 7.1.4.24, 7.5.4.2
Setpoints, 10 CFR 50.55a(h)	7.1.4.25
TMI-Related Requirements, 10 CFR 50.34(f)	7.5.4.1
Diversity and Defense-in-Depth, 10 CFR 50.55a(h) and GDC 22	7.1.4.21, 7.8
Inspections, Tests, Analyses, and Acceptance Criteria, 10 CFR 52.47(b)(1)	14.3.5

10 CFR 50.55a(a)(3) allows an applicant under 10 CFR Part 52 to propose alternatives to the requirements of 10 CFR 50.55a(h). The U.S. EPR design certification applicant proposes to use IEEE Std 603-1998, as an alternative to 10 CFR 50.55a(h), which requires the use of IEEE Std 603-1991. Section 7.1.4.1.1 of this report discusses the staff's evaluation and approval of this alternative.

The staff's evaluation on the ESF systems presented in this section is based on IEEE Std 603-1998, and the scope of the evaluation is limited to Section 4, "Design Bases," in IEEE Std 603-1998 and the applicable GDC.

The staff's review of the ESF system conducted in this Section is based on the docketed FSAR Revision 2. However, since the FSAR Revision 2 was submitted, the applicant made several changes to the I&C system design as part of RAI responses. Those changes were incorporated as mark-ups in FSAR Tier 1, Section 2.4, and FSAR Tier 2, Chapter 7, Interim Revision 3. Specifically, the June 22, 2011, response to **RAI 452, Question 07.03-36, and RAI 442, Question 07.03-32**, provide FSAR Tier 1 and 2, Interim Revision 3 mark-ups that **will be tracked as confirmatory items**.

#### 7.3.4.1 *System Description*

There are four divisions of redundant ESF logic that are part of the four divisions of overall PS actuation logic. The automatic actuation of ESF systems and auxiliary supporting systems is performed by the PS when selected plant parameters reach the appropriate setpoints. These automatic actuation orders are sent to the PACS for prioritization and interface to the actuators. For details on the staff's review of the PACS, refer to Section 7.1 of this report. The ESF actuation sequences performed by the PS are illustrated in FSAR Tier 2, Figure 7.3-1, and in Technical Report ANP-10309P, "U.S. EPR Protection System Technical Report," Figure 8-1, Revision 3.

##### 7.3.4.1.1 *ESF Automatic Actuation*

Each division of ESF logic contains five APUs. There are two subsystems in each division. One subsystem includes two APUs and the other has three APUs. The APU acquires one fourth of the redundant sensor measurements that are inputs to a specified ESF actuation function. The APU in each division performs any signal processing using the measurements

acquired by that division (e.g., filtering, range conversion, calculations). After the signal is processed, the APU compares the processed variable to its corresponding setpoint. The APU also proceeds to compare processed variables to the relevant actuation setpoint in the other three divisional APUs. If a setpoint is exceeded, the APU in that division generates a partial trigger signal for the appropriate ESF function.

Downstream of the APU in the ESF actuation sequence are the ALUs. Each division of ESF logic contains four ALUs. Each of the two subsystems in a division includes two redundant ALUs. Two-out-of-four voting logic is performed in each ALU on the partial trigger signals from all four divisions. If the voting logic is satisfied, an actuation order is generated. If any additional logic is needed (e.g., comparison to permissive conditions), the ALU performs this logic. The partial trigger signals from each division's APU are sent to both ALUs in the PS division responsible for the associated actuation. The actuation signal is latched via a set reset function block in the ALU to confirm completion of the function. The actuation signals of the redundant ALU in each subsystem are combined in hardwired "OR" configuration so that either redundant unit can actuate the function.

Once an actuation signal is generated from either ALU, the signal is sent to the PACS module associated with each actuator required for the function. Each ESF actuator can receive actuation orders from multiple I&C systems. Therefore, the PACS is used to prioritize the actuation orders. The PACS collects the actuation signals from multiple I&C systems and transfers the proper actuation order to the actuator according to predefined priority assignments. The exception to this is the turbine trip function, which is received by the associated turbine control system and does not involve a PAC module.

The SAS performs closed loop automatic controls of certain ESF systems following ESF actuation initiated by the PS and also provides safety interlock functions. These controls are described in FSAR Tier 2, Section 7.3.1.2, "Engineered Safety Features Actuation Functional Descriptions," with their associated actuation functions. The SAS is described in FSAR Tier 2, Section 7.1.

#### *7.3.4.1.2 ESF System Manual Actuation*

The capability for manual system-level ESF actuations is available to the operator through the SICS, in the MCR. The manual actuations and the corresponding automatic ESF functions are described in FSAR Tier 2, Section 7.3.1.2. FSAR Tier 2, Figure 7.3-1, Sheet 2 of 5, Interim Revision 3 mark-ups, provides the ESF manual actuation sequence. The manual actuation signals from the SICS are acquired by the ALUs of the PS and are combined with the automatic actuation logic for the corresponding automatic ESF function.

The capability for component-level control of ESF system actuators is available to the operator on both the PICS and the SICS in the MCR. Commands from the PICS are processed by the PAS and sent to the PACS for prioritization. Commands from the SICS are sent directly, via hardwired connection, to the PACS for prioritization. SICS is the safety-related actuation path and PICS is the non-safety-related actuation path. The capability for manual reset of sense and command ESF actuation outputs is only provided on the SICS. Not all ESF actuations require a manual reset. There are cases where a sense and command output is cleared after the PS determines that the initiating condition has cleared. The reset functionality related to each ESF actuation is described in FSAR Tier 2, Section 7.3.1.2. A more detailed description of the operation of the SICS and PICS is presented in FSAR Tier 2, Sections 7.1.

#### *7.3.4.1.3 Voting Logic in ALUs*

In the presence of a single failure or multiple failures upstream of the ALU layer, the system modifies the normal voting logic to take into account any faulty signal(s) if an ESF actuation is required. Each ESF actuation function is evaluated on a case by case basis to determine whether the vote is modified toward actuation or no actuation. In the case where an inadvertent actuation of ESF could challenge plant safety, the function is modified toward no actuation.

Otherwise, the function is modified toward actuation. The concept of modification toward actuation is described in Technical Report ANP-10309P, Section 7.2. The concept of modification toward no actuation based on the number of input signals to the voting function block that carry a faulty status is as follows:

- Zero faulty input signals present is interpreted as a vote of 2/4 (normal logic)
- One faulty input signal present will result in a modified actuation voting logic of 2/3
- Two faulty input signals present will result in a modified actuation voting logic of 2/2
- Three faulty input signals present will result in no ESF actuations
- Four faulty input signals present will result in no ESF actuations

Technical Report ANP-10309P, Section 7.3 describes the methods used to mark an invalid signal with a faulty status before reaching the voting function. An evaluation of voting logic as it pertains to single failure criterion, IEEE Std 603-1998, Clause 5.1, is addressed in Section 7.1.4.5 of this report.

#### *7.3.4.2 Evaluation of Design Bases*

The objective of the staff's review of FSAR Tier 2, Section 7.3, is to ensure that the design of ESF will perform all required safety functions for all ranges of plant conditions. Compliance to all applicable NRC regulations is measured utilizing a set of acceptance criteria found in SRP Section 7.3.

##### *7.3.4.2.1 Design Basis Events and Protective Actions*

IEEE Std 603-1998, Clause 4.a, requires, in part, the design basis events applicable to each operating mode along with initial conditions and allowable limits for each event to be documented. The staff used SRP Appendix 7.1-C as guidance in the review of conformance to IEEE Std 603-1998, Clause 4.a. FSAR Tier 2, Section 7.3.2.1.1, "Design Basis: Applicable Events (Clause 4.a and 4.b of IEEE Std 603-1998)," discusses design basis event documentation. FSAR Tier 2, Section 7.3.2.1.1, points to FSAR Tier 2, Chapter 15, for information that provides conformance to IEEE Std 603-1998, Clause 4.a. The design basis events for the U.S. EPR are listed in FSAR Tier 2, Table 15.0-1. Initial conditions for each event are analyzed and shown in FSAR Tier 2, Table 15.0-6, "Reactivity Coefficients, Scram Reactivity, and Computer Codes." ITAAC for the PS is provided in FSAR Tier 1, Section 2.4.1, which lists the ESF protective functions for the design basis events in FSAR Tier 1, Table 2.4.1-3, "Protection System Automatic Engineered Safety Features and Input Variables." Based upon the review of the system design for conformance to this requirement, the staff concludes that the applicant provided a sufficient level of detail to adequately address the

requirements of IEEE Std 603-1998, Clause 4.a, and the requirements of 10 CFR 52.47(b)(1) for verification of this aspect of the U.S. EPR design.

IEEE Std 603-1998, Clause 4.b, requires the safety functions and corresponding protective actions of the execute features for each design basis event be documented. Additionally, GDC 20 requires, in part, that the protection systems be designed to sense accident conditions and to initiate the operation of systems and components important to safety. The staff used SRP Appendix 7.1-C as guidance in the review of conformance to IEEE Std 603-1998, Clause 4.b. Compliance for IEEE Std 603-1998, Clause 4.b is discussed in FSAR Tier 2, Section 7.3.2.1.1. FSAR Tier 2, Section 7.3.2.1.1, points to FSAR Tier 2, Table 15.0-10, as the location for specific ESF actuations with the corresponding design basis events for which they are designed to mitigate. Detailed information on specific ESF actuations are also discussed in FSAR Tier 2, Sections 7.3.1.2.1 through 7.3.1.2.18.

Table 7.3-2 below shows the design basis events documented in Chapter 15 and the corresponding protective functions and process variables and ranges for the input signals for the corresponding protective functions, as documented in FSAR Tier 2, Section 7.3.

**Table 7.3-2 ESF Actuation Functions**

[Source: FSAR Tier 2, Table 7.3 1, Interim Revision 3 mark-ups]

Protection Function	Design Basis Event	Variables to Be Monitored	Range of Variables
Safety Injection System Actuation	Loss of Coolant Accident	Pressurizer Pressure (NR)	1,615 – 2,515 psia
		Hot Leg Pressure (WR)	15 – 3,015 psia
		Hot Leg Temperature (WR)	32°F – 662°F
		Hot Leg Loop Level	0 – 30.71 in.
Reactor Coolant Pump Trip	Small Break Loss of Coolant Accident	RCP Differential Pressure	0 – 120% nominal
EFW System Actuation (EFWS)	Loss of Main Feedwater	SG Level (WR)	0 – 100% MR
EFW System Isolation	SG Tube Rupture (SGTR)	SG Level (WR)	0 – 100% MR
SG Isolation	SG Tube Rupture	Main Steam (MS) Line Activity	$1 \times 10^{-1}$ – $1 \times 10^4$ counts/sec.
		SG Level (NR)	0 – 100% MR

Protection Function	Design Basis Event	Variables to Be Monitored	Range of Variables
Main Steam Relief Isolation Valve Opening	Loss of Secondary Heat Sink/High SG Pressure	SG Pressure	15 – 1,615 psia
Main Steam Relief Isolation	Low SG Pressure condition	SG Pressure	15 – 1,615 psia
Main Steam Isolation	Steam or Feedwater System Piping failure	SG Pressure	15 – 1,615 psia
		SG isolation signal	N/A
		Containment equipment compartment pressure	-3 to +7 psig
		Containment service compartment pressure (NR)	-3 to +7 psig
Main Feedwater Isolation	Loss of SG Level Control and RCS Overcooling Following RT	SG Level (NR)	0 – 100% MR
		SG Pressure	15 – 1,615 psia
		Containment equipment compartment pressure	-3 to +7 psig
		Containment service compartment pressure (NR)	-3 to +7 psig
Containment Isolation	Loss of Coolant Accident	Containment Service Compartment Pressure (NR)	-3 to +7 psig
		Containment Service Compartment Pressure (WR)	-5 to +220 psig
		Containment Equipment Compartment Pressure	-3 to +7 psig
		Containment High Range Activity	$1 \times 10^{-1}$ – $1 \times 10^7$ Rad/hr
Emergency Diesel Generator Actuation	Loss of Offsite Power	6.9 kV Bus Voltage	0 – 8.625 kV
Pressurizer Safety Relief Valve (PSRV) Opening	Brittle Fracture Protection due to LTOP Condition	Hot Leg Pressure (NR)	0 -870 psia



Protection Function	Design Basis Event	Variables to Be Monitored	Range of Variables
Chemical and Volume Control System (CVCS) Charging Isolation.	CVCS Malfunction Leading to Pressurizer Overfill and Opening of the PSRVs.	Pressurizer Level (NR)	0 – 100% MR
CVCS Isolation for Anti-Dilution	RCS Boron Concentration Dilution	Boron Concentration	0 – 5,000 ppm
		CVCS Charging Flow	0 – 320,000 lb/hr
		Cold Leg Temperature (WR)	32 °F – 662 °F
MCR A/C Isolation and Filtering	High Activity from Any Design Basis Event or Stage One Containment Isolation	MCR Air Intake Duct Activity	$1 \times 10^{-5}$ – $1 \times 10^1$ Rad/hr
Turbine Trip on Reactor Trip	Reactor Trip	RT Initiated Signal	N/A
Partial Cooldown Actuation	SIS Actuation due to a Design Basis Event	SIS Actuation Signal Generated	N/A
Hydrogen Mixing Dampers (HMD) Opening	This Actuation Provides for Convection and Atmospheric Mixing in the Event of a Design Basis Event Which Could Result in the Release of Hydrogen into the Containment Building.	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
		Cont. Equipment Compartment and Cont. Service Compartment Differential Pressure	-7.25 to +7.25 psi

In a June 9, 2011, response to RAI 442, Question 07.03-32, the applicant provided Interim Revision 3 mark-up of FSAR Tier 2, Section 7.3. The staff observed the following additional changes in Table 7.3-1, “ESF Actuation Variables” that were not the result of the staff’s question as documented in RAI 442, Question 07.03-32:

- For the CVCS isolation for anti-dilution protective function, boron temperature was removed from the list of variables monitored for this function in Interim Revision 3 of the FSAR. FSAR Tier 2, Figure 7.3-22, that depicts this function, does not show boron temperature being deleted as a change for Interim Revision 3. Interim Revision 3 mark-up of the FSAR for Section 7.3.1.2.11 does not describe boron temperature as an input variable and does not show any revision concerning this deletion. Revision 2 of FSAR Tier 2, Section 7.3, shows boron temperature as an input variable on Figure 7.3-22. FSAR Tier 2, Table 7.3-1 also shows boron temperature as a monitored variable.
- Turbine trip protective function was deleted.

- For MFWS isolation protective function, RT breaker position was deleted. Also, SG isolation signal was not included. FSAR Tier 2, Figure 7.3-16, depicts the MFWS isolation function. RT initiation is shown as an input variable while SG isolation signal is not shown. Interim Revision 3 mark-up of FSAR Tier 2, Section 7.3.1.2.8, describes both the initiation of RT and SG isolation signal as initiating conditions for MFWS isolation.

FSAR Tier 2, Table 7.3-1, provided a summary of the ESF protective functions and the associated initiating conditions while showing information on the monitoring range of each variable used. However, the staff is seeking to clarify why the above changes to FSAR Tier 2, Table 7.3-1 were made. Therefore, in RAI 505, Question 07.03-37, the staff requested that the applicant address this issue. **RAI 505, Question 07.03-37 is being tracked as an open item.**

FSAR Tier 1, Section 2.4.1, states that the PS performs automatic initiation of ESF functions. PS ITAAC, FSAR Tier 1, Interim Revision 3 mark-up, Table 2.4.1 3, identifies the same protective functions and the corresponding input variables as FSAR Tier 2, interim Revision 3 mark-up. Table 7.3-1. ITAAC Item 4.2 provides the commitment from the applicant that the PS generates automatic ESF signals based on information provided in FSAR Tier 2, Revision 3, Table 2.4.1-3. The staff finds that the FSAR Tier 1 design information and associated ITAAC meets the requirements of 10 CFR 52.47(b)(1) for verification of this aspect of the FSAR.

#### *7.3.4.2.2 Permissives and Monitored Variables*

IEEE Std 603-1998, Clause 4.c, requires documentation of the permissive conditions for each operating bypass capability that is to be provided. The staff used SRP Appendix 7.1 C as guidance in the review of conformance to IEEE Std 603-1998, Clause 4.c. Permissive signals are used to enable, disable, or modify the operation of ESF functions based on existing plant conditions. If operator action is required to validate or inhibit a permissive signal after the corresponding plant condition, then it is denoted as "Manual." Otherwise, the permissive is automatically validated or inhibited by the PS.

FSAR Tier 2, Section 7.3.2.1.2, "Design Basis: Permissive Conditions for Operating Bypasses (Clause 4.c of IEEE Std 603-1998)," discusses the conformance of the U.S. EPR design to IEEE Std 603-1998, Clause 4.c. The operating bypass conditions, as they relate to ESF, are described in FSAR Tier 2, Sections 7.3.1.2.1 through Section 7.3.1.2.18. A detailed discussion on the development of each permissive signal is described in FSAR Tier 2, Section 7.2.1.3. A discussion on the staff's review of permissive signals and conditions is discussed in Section 7.2 of this report. The permissive conditions are also documented in the PS ITAAC located in FSAR Tier 1, Section 2.4. In RAI 78, Question 14.03.05 4, the staff requested that the applicant clarify the ITAAC and to explain how compliance with IEEE Std 603-1998, Clause 4.c was being addressed. Table 7.3-3 below contains a summary of existing permissives and their associated conditions based upon information the applicant provided with its June 12, 2009, response to RAI 78, Question 14.03.05 4, including their proposed revisions to the FSAR as amplified by the information provided with the FSAR Tier 2, Interim Revision 3 mark-up, Section 7.2.

**Table 7.3-3 Permissives and Operating Bypasses**

Permissives	Inhibit	Validate	Permissive Conditions	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P2	Automatic	Automatic	Permissive is representative of PRD neutron flux measurements higher than a low-power setpoint value (10% power). The P2 setpoint value corresponds to the value below which transients do not lead to risk of DNB	Low DNBR RT	
				HLPD RT	
				Low RCS Loop Flow RT	
				Low RCP Speed RT	
				Low Pressurizer Pressure RT	
P3	Automatic	Automatic	Permissive is representative of PRD neutron flux measurements higher than an intermediate power setpoint value (70% power). The P3 setpoint value corresponds to value below which loss of one reactor coolant pump does not lead to risk of DNB.	Low-Low RCS Loop RT	

Permissives	Inhibit	Validate	Permissive Conditions	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P5	Automatic	Automatic	Permissive is representative of IRD neutron flux measurements above a low-power setpoint value ( $10^{-5}$ percent power). The P5 setpoint value corresponds to boundary between the operating ranges of the source range detectors and intermediate range detectors.	High Core Power Level RT	
				Low Saturation Margin RT	
P6	Automatic	Manual	Permissive is representative of core thermal power above a low-power setpoint value (10% power) corresponding to the boundary between the operating ranges of the IRDs and the PRDs.		High Neutron Flux RT
					Low Doubling Time RT
P7	Automatic	Automatic	Permissive defines when reactor coolant pumps are no longer in operation.	CVCS Isolation on ADM at Standard Shutdown Conditions	CVCS Isolation on ADM at Shutdown Conditions
				CVCS Isolation on ADM at Standard Shutdown Conditions with Manual Calculation	

Permissives	Inhibit	Validate	Permissive Conditions	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P8	Automatic	Automatic	Permissive defines the shutdown state with all rods in.	CVCS Isolation on ADM at Power	CVCS Isolation on ADM at Standard Shutdown Conditions
					CVCS Isolation on ADM at Standard Shutdown Conditions with Manual Calculation
P12	Automatic	Manual	Permissive facilitates plant heatup and cooldown by disabling certain ESF functions.		High Pressurizer Level RT
					Low Hot Leg Pressure RT
					Low SG Pressure RT
					Main Steam Relief Train (MSRT) Isolation (manual)
					MSRT Isolation (low SG pressure)
					Main Steam Isolation (low SG pressure)
P13	Automatic	Manual	Permissive defines when SG draining and filling operations are allowed.		MFW Startup and Shutdown System (SSS) Isolation (low SG pressure)
					Low SG Level RT
					High SG Level RT
					EFWS Actuation (low SG level)
					EFWS Actuation (SIS + loss of offsite power (LOOP))
					EFWS Actuation (manual)

Permissives	Inhibit	Validate	Permissive Conditions	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
					EFWS Isolation (high SG level)
					MFW Full Load Isolation (high SG level)
					MFW SSS Isolation (high SG level for period of time + RT)
					SG Isolation
P14	Manual	Manual	Permissive defines when the residual heat removal system is allowed to be connected to the RCS.		Partial Cooldown Actuation
P15	Automatic	Manual	Permissive defines when SI actuation due to $\Delta P_{sat}$ is disabled and SI actuation due to low loop level is enabled.		SIS Actuation (low delta Psat)
					SIS Actuation (low RCS loop level)
P16	Manual	Manual	Permissive defines when the SIS may be aligned from cold leg injection to hot leg injection.		Align SIS from cold leg injection to hot leg injection
P17	Automatic	Manual	Permissive corresponds to the cold leg temperature conditions where brittle fracture protection is required.	PSRV Opening	CVCS Charging Isolation (high Pressurizer level)
P18	Automatic	Automatic	Permissive prevents the unsafe positioning of the SG transfer		Repositioning of SG transfer valves

Permissives	Inhibit	Validate	Permissive Conditions	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
			valves.		

The above table presents a complete description of what existing operating bypasses and associated permissives that will be tested under the PS ITAAC. The staff issued RAI 78, Question 14.03.05-4, which addressed, in part, proper operation of permissive signals and the applicant presented supporting ITAAC information in their June 12, 2009, response. The staff confirmed that the information was added to FSAR Tier 1, Revision 2, Section 2.4, and is accurate and complete. FSAR Tier 1, Section 2.4.1 states that the PS generates permissive signals that authorize the activation or deactivation of certain protective functions based on plant conditions. The PS ITAAC, Table 2.4.1 5 identifies the same PS permissives and the corresponding operating bypasses as Table 7.3-3 of this report, which is based on design information in FSAR Tier 2, Revision 2, Section 7.3. ITAAC Item 4.3 in FSAR Tier 1, Table 2.4.1-7 provides the commitment from the applicant that the PS provides permissives for operating bypasses capability for certain PS signals based on information provided in FSAR Tier 2, Revision 2, Table 2.4.1-5.

Therefore, the staff finds that the applicant adequately addressed the requirements of IEEE Std 603-1998, Clause 4.c, and 10 CFR 52.47(b)(1) by clearly documenting the permissive conditions for operating bypasses provided in the FSAR and provided sufficient ITAAC to verify the permissive operation.

#### *7.3.4.2.3 Variables Used for Automatic or Manual Protective Actions*

IEEE Std 603-1998, Clause 4.d, requires, in part, that the FSAR document the variables or combinations of variables used by the ESF actuation system to be monitored manually or automatically. Also, IEEE Std 603-1998, Clause 4.d requires the applicant to document the analytical limit associated with each variable, the ranges and rates of change of these variables until completion of protective action is ensured. Guidance from SRP Appendix 7.1-C states the information as described in IEEE Std 603-1998, Clause 4.d be provided. In addition, SRP Section 7.1-C also identifies the need for the applicant to document system accuracies and response times that verify ESF ability to properly address the accident analyses in FSAR Tier 2, Chapter 15, based upon the documented variables. The applicant describes conformance to IEEE Std 603-1998, Clause 4.d in FSAR Tier 2, Section 7.3.2.1.3. FSAR Tier 2, Table 7.3-1, "ESF Actuation Variables," contains a list of the ESF actuation system variables with respect to their associated protective functions, including the range of each variable. The applicant discussed compliance with Clause 4.d in FSAR Tier 2, Section 7.1.2.6.3, Interim Revision 3 mark-ups. GDC 20 requires, in part, that the PS design automatically initiate systems that will prevent fuel design limits from being exceeded during an accident, sense accident conditions, and initiate the operation of systems and components important to safety. The applicant discussed the compliance with GDC 20 in FSAR Tier 2, Section 7.1.2.2.9.

In the initial review, FSAR Tier 2, Section 7.3 did not document response times. In RAI 60, Question 07.03-11, the staff requested that the applicant provide this information. In a June 12, 2009, response to RAI 60, Question 07.03-11, the applicant stated that ESF response times are documented in FSAR Tier 2, Table 15.0-8, "Engineered Safety Features Functions Used in the Accident Analysis," and the PS response times will be tested and verified according to the

ITAAC documented in FSAR Tier 1, Table 2.4.1-7, Item 4.24, and FSAR Tier 2, Section 14.2.12.11.22, Test No. 146, of the initial test program (ITP).

The staff reviewed the applicant's June 12, 2009, response to RAI 60, Question 07.03-11, and determined it inadequate for the following reasons:

- Table 15.0-8 shows "Time Delays" associated with each ESF function used in the accident analysis. However, Startup Test No. 146 is for the PS and does not specifically test for ESF response times or accuracies.
- In addition, the section in which the applicant identifies the location of Test No. 146 is incorrect. In FSAR Tier 2, Revision 2, Test No. 146 is located in FSAR Tier 2, Section 14.2.12.11.22. Test No. 146 does not specifically test the ESF functions, but is focused on testing of the reactor trip features of the PS.

Based upon the review of the applicant's response, the staff created follow-up RAI 285, Question 07.03-25. In a February 26, 2010, response to RAI 285, Question 07.03-25, the applicant committed to adding specific testing for ESF response times to support the Chapter 15 accident analyses. Specifically, the applicant stated:

The bounding PS response times discussed in the Second Request for Additional Information for ANP 10281(P), Attachment B are in conformance with the response time assumptions used in the accident analysis and given in FSAR Tier 2, Table 15.0-7 and Table 15.0-8. If needed, AREVA NP can provide supporting documentation, such as a function by function demonstration of consistency, for NRC audit. Refer to FSAR Tier 1, Section 2.4.1, Item 4.24, and associated ITAAC, which has been added in the response to RAI 285 Supplement 4, Question 07.03-25 and addresses verification that the PS response times support accident analysis assumptions.

The Second Request for Additional Information for Technical Report ANP 10281(P), Attachment B, states:

The total response time for a specified function consists of several sub intervals that span from a process variable exceeding a pre-defined limit to completion of the protective function. The sub-interval addressed herein accounts for the computerized portion of the protection channel and is defined as the time from sensor conditioning output to RT breaker input terminals for RT functions, or to input terminals of the PACS for ESF actuation functions.

The PACS is not included in the PS response time analysis. Time delays introduced by the priority module in the PACS are included with the response time of the actuator it controls and is verified through response time testing of the actuator.

FSAR Tier 2, Chapter 15, Table 15.0-8, Note 4 states the time delays (response times):

....represents the total time for completion of the function. Includes sensor delay, I&C delay, and other delays as noted until the function is completed.

The applicant stated that the PACS is not included in the response times. This is in conflict with the definition of the response times for completion of ESF actuation in FSAR Tier 2, Chapter 15. The Chapter 15 definition makes no distinction between the computerized portions of the PS



and the PACS, and implies that the response times would envelope all timing delays from sensor to final actuation device. It should also be noted that the PACS ITAAC in FSAR Tier 1, Section 2.4.5, "Priority and Actuator Control System," makes no mention of response timing. For example, EFW is an ESF, and the ITAAC for EFW is in FSAR Tier 1, Section 2.2.4, "EFW System." There is no mention of response timing, in terms of valve stroke time with the PACS module, in the ITAAC. There is also no mention of response time testing in order to meet the bounding times of the Chapter 15 safety analyses. This is in conflict with the applicant's statement in its February 26, 2010, response to RAI 286, Question 07.09-47. In RAI 286, Question 07.09-47, the staff requested that the applicant present the estimated response times of the PS and demonstrate how they are bounded by the 'time delays' presented in FSAR Tier 2, Table 15.0-7 and Table 15.0-8 for the accident analyses. In a February 26, 2010, response to RAI 286, Question 07.09-47, the applicant stated:

The total response time for a given function consists of several sub-intervals that span from a process variable exceeding a pre-defined limit to completion of the protective function. The sub-interval addressed herein accounts for the computerized portion of the protection channel and is defined as the time from sensor conditioning output to RT breaker input terminals for RT functions, or to input terminals of the PACS for ESF actuation functions." The PACS is not included in the PS response time analysis. Time delays introduced by the priority module in the PACS are included with the response time of the actuator it controls and is verified through response time testing of the actuator.

If the response timing of the PACS is not included in the PS, PACS, or any other FSAR Tier 1 ITAAC, then the staff is not able make a reasonable assurance finding that the as-built configuration of the PS will meet the bounding response times of the Chapter 15 safety analyses. In RAI 414, Question 07.03-30, the staff requested that the applicant clarify this issue. **RAI 414, Question 07.03-30 is being tracked as an open item.**

The applicant also provided Interim Revision 3 mark-up of FSAR Tier 2, Table 15.0-8, which shows the revised notes detailing that the time delays on the ESF function tables include PACS delays. In RAI 452, Question 07.03-35 the staff requested that the applicant describe how single failures identified in the Protection System (PS) system-level FMEA in Section 7.3 correlate to pre-defined failure states. In a March 29, 2011, response to RAI 452, Question 07.03-35, the applicant provided an Interim Revision 3 mark-up for FSAR Tier 2, Section 14.2.12.11.22, Test No. 146. The revised Test No. 146 identifies the testing of PS response times. FSAR Tier 1, Section 2.4.1, of Interim Revision 3 mark-ups was submitted with RAI 452, Question 07.03-36, but included information that supports RAI 452, Question 07.03-35. This section of the interim revision 3 mark-ups identifies that the PS response time for ESF signals is less than the value required to satisfy the accident analyses. PS ITAAC in Table 2.4.1-7, Item 4.24, also provided with the RAI 452, Question 07.03-36 response submittal provides the applicant's commitment for verifying the response times for ESF. The staff finds the applicant's responses acceptable. The applicant clearly stated that the PACS modules would be included in response time testing and therefore included under the PS ITAAC, as well as, periodic response time testing as performed during surveillance testing as described in Technical Report ANP-10315P, "U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring," Revision 1. The staff will verify the incorporation of the above material in the final Revision 3 of the FSAR. RAI 452, Question 07.03-36 is being tracked as a confirmatory item.

#### 7.3.4.2.4 *Manual ESF System Actuation*

The staff evaluated conformance to IEEE Std 603-1998, Clause 4.e, which requires, in part, that the application show:

- The points in time and plant conditions during which manual control is allowed
- The justification for permitting initiation or control subsequent to initiation solely by manual means
- The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations shall be performed
- The variables in IEEE Std 603-1998, Clause 4.d that shall be displayed for the operator to use in taking manual action.

The staff used SRP Appendix 7.1 C.5, "Safety System Criteria (IEEE Std 603 1991 Clause 5)," and BTP 7- 6, "Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode," as guidance for this portion of the evaluation. The applicant states that documentation of conformance to IEEE Std 603-1998, Clause 4.e is located in FSAR Tier 2, Section 7.3.2.1.4, "Design Basis: Manual ESF System Actuation (Clause 4.e of IEEE Std 603 1998)." Specifically, FSAR Tier 2, Section 7.3.2.1.4, addresses IEEE Std 603-1998, Sub clauses 4.e.2 and 4.e.3. The capability for manual system level actuation of ESF functions is available to the operator as described in FSAR Tier 2, Section 7.3.1.1, "System Description." The function specific implementation of system level actuation is described for each function in FSAR Tier 2, Sections 7.3.1.2.1 through 7.3.1.2.18. In a June 12, 2009, response to RAI 60, Question 07.03-12, which asked, in part, when manual control is available and which variables would be displayed for the operator to use in taking manual action, the applicant stated that the information concerning when manual control is allowed, as well as display variables (IEEE Std 603-1998, Sub clauses 4.e.1 and 4.e.4, respectively), is addressed as part of the U.S. EPR Human Factors Program. The U.S. EPR Human Factors Program is evaluated in Chapter 18, "Human Factors," of this report. Also, in a June 12, 2009, response to RAI 78, Question 14.03.05-4, which asked in part which ITAAC address the specific IEEE Std 603-1998 criteria, the applicant provided an ITAAC mapping scheme to identify where the applicant discusses compliance with the applicable regulations and standards, including IEEE Std 603-1998.

FSAR Tier 2, Section 15.0.3.7, "Main Steam Line Break Outside of Reactor Building Accident," states that operator actions are credited for isolating an affected SG during an (SGTR event. FSAR Tier 2, Section 7.3.1.2.14, "SG Isolation," describes how the PS automatically performs an isolation of an affected steam generator during an SGTR) The description in FSAR Tier 2, Section 7.3, did not address crediting of manual actions for a SGTR event. In particular, it is not explicitly documented in FSAR Tier 2, Section 7.3 that the manual controls for the ESF systems used to mitigate a SGTR are safety-related and utilize safety-related displays and controls. For the U.S. EPR design, the safety-related control panel would be the SICS. The applicant stated previously that normal activities and accident mitigation activities conducted by plant operators will be performed on the PICS. In follow up RAI 285, Question 07.03-27, the staff requested that the applicant clarify why credit is being taken for manual SG isolation in the accident analyses for a SGTR when automatic mechanisms are available. In a February 19, 2010, response to RAI 285, Question 07.03-27, the applicant provided the following information:

FSAR Tier 2, Section 7.1.2.6.29 describes compliance with IEEE Std 603-1998 Clause 6.2.b. AREVA NP acknowledges that Section 7.1.2.6.29 provides reference to Section 7.3 for manual controls credited in the accident analyses, and that Section 7.3 does not specifically acknowledge manual actions credited in the accident analysis. Therefore, Section 7.3 will be revised to clarify this point.

The applicant committed to revising the FSAR to clarify this point and to clarify that manual controls used to mitigate an SGTR exist on the SICS. The variables used to identify an SGTR are documented in FSAR Tier 2, Tables 7.3 1 and 15.0 8. The staff reviewed the applicant's proposed FSAR mark-ups included in the February 19, 2010, response to RAI 285, Question 07.03-27, and finds them to be adequate. The applicant also stated that the SGTR is a relatively slow-moving event and does not require mitigation within the first 30 minutes following the occurrence of a rupture. The applicant states that the decision not to take credit for automatic isolation functions in the safety analysis includes the following rationale:

- The nature of the event (slow progression and the range of possible plant responses) makes it difficult to determine exactly when the automatic function would be actuated.
- If the automatic function were to initiate prior to 30 minutes, the event results are more favorable.
- The slow progression of the event allows credit to be taken for manual actions after 30 minutes.

The applicant also provided this scenario as an example for why automatic isolation is not credited:

U.S. EPR design includes an automatic feature that performs the SG isolation in the presence of either a steam line high activity or high steam level coincident with the initiation of partial cooldown. A Safety Injection (SI) signal initiates partial cooldown. The high activity signal under potential scenarios varies as does the timing of SI in each scenario. For example, if the CVCS continues to function, it can provide sufficient make up for the loss of inventory through the ruptured tube. In this case the operator follows the emergency operating procedures (EOP) to manually trip the reactor or maneuver the plant through a controlled shutdown. Under this condition, although the high steam line activity signal may be present, SI or high SG level may be significantly delayed, resulting in a delay to isolate the affected SG and challenging offsite dose limits. In contrast, if CVCS is not available the reactor automatically trips following the SGTR and a SI signal occurs shortly after reactor trip. The SI signal initiates partial cooldown and in combination with high steam line high activity automatically isolates the affected SG. The single failure evaluated (e.g., stuck open MSRT) could also impact the timing of SI.

An SGTR event can become a non-linear evolution that is not easily bounded by automatic isolation, considering the numerous circumstances that can be coincident with the event. It should also be noted that this practice conforms to current industry practices for mitigation of a SGTR. The staff agrees with the rationale the applicant presented. In RAI 442, Question 07.03-32, the staff requested that the applicant explicitly state in FSAR Tier 2, Section 7.3, which ESF functions have manual credited functions in the safety analysis in FSAR Tier 2,

Chapter 15, and state the existence of manual, component level controls available in the MCR on both PICS and SICS. In a June 9, 2011, response to RAI 442, Question 07.03-32, the applicant provided Interim Revision 3 mark-ups of FSAR Tier 2, Section 7.3 and Chapter 15, to reflect these changes. In the mark-ups for FSAR Tier 2, Section 7.3, the applicant identifies manual controls under specified ESF functions that are credited in the accident analysis.

The applicant also identified in the Interim Revision 3 mark-ups of Section 7.3 that component level manual controls are available in the MCR on the PICS and SICS. The applicant identified this information for each ESF function. In the Interim Revision 3 mark-ups of Chapter 15, the applicant clarified that the system-level manual controls are credited in the safety analysis. The staff reviewed these changes and finds them adequate.

#### *7.3.4.2.5 Spatially Dependent Variables*

The staff verified conformance to IEEE Std 603-1998, Clause 4.f, which requires the identification of the minimum number and location of sensors for variables that are spatially dependent. The staff used SRP Appendix 7.1 C as guidance in the review of conformance to IEEE Std 603-1998, Clause 4.f. According to FSAR Tier 2, Section 7.3.2.1.5, "Design Basis: Spatially Dependent Variables (Clause 4.f of IEEE Std 603-1998)," the U.S. EPR design does not use any spatially dependent variables as input to any ESF actuations. The staff agrees that there are no spatially dependent variables used for ESF actuations and finds that the applicant has adequately addressed the requirements of IEEE Std 603-1998, Clause 4.f, for the I&C portion of the ESF.

#### *7.3.4.2.6 Protection System Reliability Methods*

IEEE Std 603-1998, Clause 4.i, requires identification of the methods used to determine that the reliability of the safety system design is appropriate and to identify methods used to verify that any qualitative or quantitative reliability goals imposed on the system design have been met. The staff used SRP Appendix 7.1 C as guidance in the review of conformance to IEEE Std 603-1998, Clause 4.i.

FSAR Tier 2, Revision 2, Section 7.1.2.6.8, documents compliance of the design to IEEE Std 603-1998, Clause 4.i. The design basis incorporates a qualitative analysis in the form of a FMEA along with a probabilistic risk assessment (PRA), which is described in FSAR Tier 2, Chapter 19, "Probabilistic Risk Assessment and Severe Accident Evaluation." The PRA is evaluated in Chapter 19 of this report. The FMEA for ESF (PS) is documented in Technical Report ANP-10309P, "U.S. EPR Protection System Technical Report," Appendix A, Revision 3. FSAR Tier 1, Table 2.4.1-7, Item 4.18, provides the applicant's commitment to perform a more detailed level PS FMEA. The staff concludes that the PS FMEA, and the PRA, adequately serve as methods to assess ESF reliability and will ensure that stated reliability goals are met; thereby satisfying the requirements of IEEE Std 603-1998, Clause 4.i and 10 CFR 52.47(b)(1).

The staff reviewed 10 CFR Part 50, Appendix A, GDC 29, and finds that this GDC has been appropriately addressed. GDC 29 states that the protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operation occurrences. The staff used SRP Appendix 7.1 A as guidance for the evaluation of this area. In this case, compliance with GDC 29 is closely tied with compliance with IEEE Std 603-1998, Clause 4.i, as the requirements for each are similar in scope. In terms of ESF, the staff finds the applicant in compliance with IEEE Std 603-1998, Clause 4.i, and as such, the requirements for GDC 29 are also met for the I&C portion of the ESF.

#### *7.3.4.2.7 Critical Points in Plant Operation That Require ESF Functionality*

IEEE Std 603-1998, Clause 4.j, requires documentation of the critical points in time or the plant conditions, after the onset of a design basis event, the point in time or plant condition for which the protective actions of the safety system shall be initiated, the proper completion of the safety function, when automatic control of protective actions are required, and plant conditions that allow returning a safety system to normal. The staff used SRP Appendix 7.1 C as guidance in the review of conformance to IEEE Std 603-1998, Clause 4.j. Statement of compliance with this requirement is discussed in FSAR Tier 2, Revision 2, Section 7.3.2.1.6. The applicant states in FSAR Tier 2, Section 7.3.2.1.6, that, as part of its commitment to meet the requirements for IEEE Std 603-1998, Clause 4.j, the accident analyses in Chapter 15 also provides a summary description of the various times and critical points that ESF functionality is necessary on a per event basis.

The applicant states the PS will initiate the ESF systems when selected variables exceed associated setpoints. The setpoints for ESF are provided to ensure the plant is protected from specified AOOs, should they arise. The safety analysis documented in FSAR Tier 2, Chapter 15, provides specific details on the plant conditions that would require ESF actuation. Based upon the review of the system design for conformance to this requirement, the staff concludes that the ESF systems conform to the requirements of IEEE Std 603-1998, Clause 4.j.

#### *7.3.4.2.8 Equipment Protective Features*

IEEE Std 603-1998, Clause 4.k, requires documentation of equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The staff used SRP Appendix 7.1 C as guidance in the review of conformance to IEEE Std 603-1998, Clause 4.k. FSAR Tier 2, Revision 2, Section 7.1.2.6.10 documents compliance of the design to IEEE Std 603-1998, Clause 4.k. However, the applicant did not explicitly state that there are no equipment protective features that can prevent a safety actuation of ESF. As such, the staff determined there was insufficient detail to finalize an evaluation for this clause. Therefore, in RAI 60, Question 07.03-14, the staff requested that the applicant clarify this issue. In a June 12, 2009, response to RAI 60, Question 07.03-14, the applicant stated that the functional requirements for the PS do not include any provisions for equipment protective features that could prevent safety functions. The applicant further stated that should the design of the PS change in the future to add such a feature, that this would be documented in conformance with IEEE Std 603-1998, Clause 4.k. The applicant did not commit to clearly stating this fact in the FSAR.

Based upon the requirements of IEEE Std 603-1998, Clause 4.k, in RAI 75, Question 07.02-3, the staff requested the applicant to clearly state in the FSAR that the current design of the U.S. EPR does not have any equipment protective features that would prevent a safety system from accomplishing its safety function. If, in the future, the design of the U.S. EPR introduces a protective feature that would prevent a safety system from accomplishing its safety function, then the applicant should take the necessary steps to document this fact in the FSAR, and the staff would review that design change. That does not alleviate the responsibility of the applicant from clearly stating in the latest FSAR revision the design aspects of the current U.S. EPR PS design with respect to IEEE Std 603-1998, Clause 4.k. In RAI 285, Question 07.03-26, the staff requested that the applicant clarify if there are no equipment protective provisions that prevent the safety systems from accomplishing their safety functions and state this clearly in the FSAR. In a February 19, 2010, response to RAI 285, Question 07.03-26, the applicant submitted its initial response by stating:

It should be noted that if a piece of safety equipment is prevented from performing its function (for example, by an equipment protective function), then a single failure has occurred. This scenario is functionally equivalent to that piece of equipment failing to perform its safety function due to any number of failure mechanisms. FMEA have been performed for the safety related process systems to demonstrate that no single failure can prevent performance of a safety function. These FMEAs are presented in the chapters of the FSAR where the process systems are described. From this perspective, it can be said that no single equipment protective function (equivalent to single failure of the equipment) can prevent performance of a safety function.

The applicant's second response provided additional information that allowed the staff to better understand the applicant's position. The staff agrees with the applicant's position that a failure to actuate due to an equipment protective feature would be bounded by the single failure analyses. However, this information should be added to the FSAR. Therefore, in follow-up RAI 414, -03 31, the staff requested that the applicant state in FSAR that there are no equipment protective features that prevent safety system actuation and provide more detail, or compensatory measures taken, if any of these features exist in the design. In a February 18, 2011, response to RAI 414, Question 07.03-31, the applicant provided the following addition to the Interim Revision 3 of FSAR Tier 2, Section 7.1:

The U.S. EPR contains equipment protective functions that may prevent a piece of safety equipment from performing its function. If a piece of safety equipment is prevented from performing its function by an equipment protective function, then a single failure has occurred. This scenario is functionally equivalent to that piece of equipment failing to perform its safety function due to any number of failure mechanisms. Failure modes and effects analysis (FMEA) have been performed for the safety-related process systems to demonstrate that no single failure can prevent performance of a safety function. Therefore, no single equipment protective function can prevent performance of a safety function.

The staff finds the above-quoted information adequately addresses the requirements of IEEE Std 603-1998, Clause 4.k. Specifically, the applicant documented the existence of these protective features in the U.S. EPR design. The applicant also stated that the U.S. EPR design can withstand this type of failure, should it occur, due to the design meeting the single-failure criterion (IEEE Std 603-1998, Clause 5.1), as demonstrated by the failure modes and effects analysis. The staff finds the applicant's mark-up submitted under RAI 442, Question 07.01-26 acceptable. Based upon a review of all materials submitted, the staff concludes that the design adequately addresses the requirements of IEEE Std 603-1998, Clause 4.k.

#### *7.3.4.2.9 Special Design Bases*

IEEE Std 603-1998, Clause 4.l, requires documentation of any special design basis imposed on the system design. The staff used SRP Appendix 7.1 C as guidance to reviewing conformance to IEEE Std 603-1998, Clause 4.l. FSAR Tier 2, Revision 2, Section 7.1.2.6.11, lists an SCCF concurrent with an AOO or PA as the special design basis imposed on the PS design. In this section, the applicant refers to FSAR Tier 2, Section 7.8, "Diverse I&C Systems," for the Diversity and Defense in Depth (D3) analysis intended to mitigate the effects of a software CCF. The staff's review of the D3 analysis is discussed in Section 7.8 of this report. The staff has not identified any other special design basis that should be imposed on the ESF design. Based

upon the review of the system design for conformance to this requirement, the staff concludes that the ESF systems conform to the requirements of IEEE Std 603-1998, Clause 4.I.

#### *7.3.4.2.10 General Design Criteria*

The staff reviewed the FSAR to verify that 10 CFR Part 50, Appendix A, GDC 10, GDC 15, and GDC 16 have been adequately addressed. GDC 10, GDC 15, and GDC 1 provide design requirements for reactor design, instrumentation and controls, RCS design, containment design and the control room, respectively. The evaluation in this section discusses GDC as they pertain to I&C. Evaluation of specific systems utilized by ESF is not within the scope of this report. The staff used SRP Appendix 7.1 A as guidance for the evaluation of this area:

- GDC 10 requires, in part, that the reactor protection system prevent reactor fuel from exceeding its specified design limits throughout all operating conditions.
- GDC 15 requires, in part, that the RCS be designed with sufficient margin to ensure that reactor coolant pressure boundary (RCPB) integrity is maintained throughout all operating conditions.
- GDC 16 requires, in part, that ESF systems ensure that reactor containment design margins are maintained throughout all operating conditions.

As described in FSAR Tier 2, Section 7.3, the design for ESF contains the following examples of features included in the ESF design to ensure compliance with GDC 10, GDC 13, GDC 15, GDC 16, and GDC 19:

- Safety Injection
- EFW
- Containment Isolation
- Pressurizer Safety Relief Valve Opening
- Main Control Room Air Conditioning System Isolation and Filtering
- System-level Manual Control on SICS
- Component-level Manual Controls on both SICS and PICS

Information on all other ESF actuations performed by the PS is described in FSAR Tier 2, Section 7.3.1.2. Design detail for DBEs and AOOs for which ESF are designed to mitigate is discussed in FSAR Tier 2, Chapter 15. The ITAAC for the protection system is documented in FSAR Tier 1, Section 2.4. FSAR Tier 1, Table 2.4.1-7, contains the ITAAC items that provide for verification that I&C portions of ESF functions will actuate and mitigate design basis accident conditions as described in the Chapter 15 safety analyses. The Initial Test Program, discussed in FSAR Tier 2, Section 14.2, also provides pre-operational testing to verify ESF design functionality. The setpoints used for ESF actuation were implemented according to an approved setpoint methodology. Section 7.1.4.26 of this report provides additional detail on the U.S. EPR setpoint program.

Based on the identification of the necessary design requirements and the verification of the actuation of the ESF based on the design basis events shown in FSAR Tier 2, Chapter 15, as well as controls being available in the MCR to manually initiate each ESF, the staff finds that the requirements of GDC 10, GDC 15, and GDC 16 have been adequately addressed in terms of ESF operation. The I&C configuration described in FSAR Tier 1, Section 2.4, and FSAR Tier 2, Section 7.3, documents an adequate level of instrumentation and controls to provide the intended protective function for each ESF.

The staff reviewed GDC 33, GDC 34, GDC 35, GDC 38, GDC 41, and GDC 44 to determine if these criteria were addressed in terms of ESF. GDC 33, GDC 34, GDC 35, GDC 38, GDC 41, and GDC 44 provide design criteria for reactor coolant make up, residual heat removal, emergency core cooling, containment heat removal, containment atmosphere clean up, and cooling water systems, respectively. The staff used SRP Appendix 7.1 A as guidance for the evaluation of this area.

- GDC 33 requires, in part, that ESF I&C systems are able to reliably initiate and control the reactor coolant makeup systems in order to mitigate the consequences of small breaks in the RCPB and maintain RCPB integrity.
- GDC 34 requires, in part, that ESF I&C systems are able to reliably initiate and control the residual heat removal systems and ensure that the ability to remove decay heat is maintained.
- GDC 35 requires, in part, that ESF I&C systems are able to reliably initiate and control the ECCS and ensure that:
- Fuel and clad damage that could interfere with continued effective core cooling is prevented
- Fuel cladding water reaction is limited to negligible amounts.
- GDC 38 requires, in part, that the ESF I&C systems are able to reliably initiate and control the containment heat removal system and ensure the ability to remove temperature and reduce pressure in containment during a loss of coolant accident is maintained.
- GDC 41 requires, in part, that the ESF I&C systems are able to reliably initiate and control the containment atmosphere control systems and ensure that containment integrity is maintained.
- GDC 44 requires, in part, that the ESF I&C systems are able to reliably initiate and control the cooling water systems and ensure that the transfer of combined heat loads from structures, systems and components important to safety, under normal and accident conditions to the ultimate heat sink is maintained.

These design criteria have been identified in FSAR Tier 2, Section 7.1.2.2.17, "GDC 33 – Reactor Coolant Makeup," through Section 7.1.2.2.22, "GDC 44 – Cooling Water," as being integrated into the design bases of ESF. In addition, the applicable IEEE Std 603-1998 requirements have also been identified in FSAR Tier 2, Section 7.1, as being integrated into ESF system design.



As stated in FSAR Tier 2, Section 7.3, the U.S. EPR design for ESF contains the following safety actuation functions:

- Safety Injection
- EFW
- Emergency Diesel Generator Actuation
- Containment Isolation
- Main Control Room Isolation/Filtration
- Partial Cooldown

The above mentioned systems are designed so that the U.S. EPR design can meet the requirements of GDC 33, GDC 34, GDC 35, GDC 38, GDC 41, and GDC 44. Within the U.S. EPR design, the PS is organized into four redundant divisions of actuation logic. Each division contains the logic necessary to individually initiate any automatic ESF actuation. In addition, each division of logic is located in a separate safeguard building. The accident analyses provided in FSAR Tier 2, Chapter 15, provides for each design basis accident and the corresponding PS actuation designed to mitigate the consequences of each accident. The PS design is in accordance with an approved quality assurance program as defined in 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants." Also, the applicant provided ITAAC for the PS in FSAR Tier 1, Section 2.4, Table 2.4.1-7. The ITAAC contains testing of system response times, setpoints, and verification of IEEE Std 603-1998 design criteria that were incorporated into overall PS design. Section 7.1.4.26 of this report provides additional detail on the U.S. EPR setpoint program. Based on the redundancy and diversity built into the design of the PS, quality requirements identified by the applicant, along with the identified ITAAC testing, the staff concludes the U.S. EPR design for the I&C portion of ESF systems meets the requirements of GDC 33, GDC 34, GDC 35, GDC 38, GDC 41, and GDC 44.

#### *7.3.4.2.11 Other Safety I&C System Compliance with Regulations*

The staff reviewed the FSAR to determine how the applicant addressed design basis requirements of IEEE Std 603-1998, Clause 4, and applicable GDCs, for SAS and other safety-related systems. The staff was unable to determine that for SAS and other safety-related system, that all design basis requirements have been incorporated. For example, in FSAR Tier 2, Section 7.1.2.6.10, Interim Revision 3 mark-ups, the applicant states that the U.S. EPR design does contain equipment protective features that may prevent a piece of safety-related equipment from performing its function and that a failure of this type would be bounded by the single failure analysis. The applicant also states the following:

Failure modes and effects analysis have been performed for the safety-related process systems to demonstrate that no single failure can prevent performance of a safety function.

The staff accepted the applicant's rationale in its evaluation of the PS for compliance with IEEE Std 603-1998, Clause 4.k in Section 7.3.4.3.8 of this report. However, the staff has not received an FMEA, or other single failure analysis, for SAS and the other safety-related systems in the U.S. EPR design. The applicant has stated compliance with IEEE Std 603-1998, Clause 4.k by

the single failure criterion but without similar analysis for SAS and other safety-systems available to the staff for review, the staff cannot make a reasonable assurance finding. If certain design basis requirements have not been incorporated, then the applicant shall provide justification for design basis requirements that have either been excluded, or are not applicable to SAS and other safety-related systems. Therefore, in RAI 505, Question 07.03-38, the staff requested that the applicant address this issue. **RAI 505, Question 07.03-38 is being tracked as an open item.**

### **7.3.5 Combined License Information Items**

No applicable items were identified in the FSAR for the ESF systems. No additional COL information items need to be included in FSAR Tier 2, Table 1.8-2, for the I&C portions of ESF.

### **7.3.6 Conclusions**

The staff reviewed the U.S. EPR engineered safety features I&C design to verify compliance with applicable regulatory requirements. During its review, the staff identified RAI 505, Questions 07.03-37 and 07.03-38, which are being tracked as open items for this section. Upon satisfactory conclusion and incorporation of the identified open item and confirmatory item question responses; and when the applicable sections within Chapters 3, 7, and 15 of the FSAR are finalized to the staff's satisfaction, the staff concludes that the design of the ESF and ESF initiation of auxiliary supporting features will be acceptable and will meet the relevant requirements of 10 CFR Part 50, Appendix A, GDC 10, GDC 15, GDC 16, GDC 33 through GDC 35, GDC 38, GDC 41, and GDC 44, as well as the requirements of 10 CFR 50.55a(h).

Based on the review of system functions in this section and Section 7.1, the staff concludes that the ESF conforms to the design bases requirements of IEEE Std 603-1998, and complies with 10 CFR 50.55(a)(h) and 10 CFR 50.34(f). The ESF setpoint methodology conforms to the guidance of RG 1.105. Based upon this review and coordination with those having primary review responsibility for the accident analysis, the staff concludes that the ESF includes the provision to sense accident conditions and anticipated operational occurrences in conformance with the accident analysis presented in FSAR Tier 2, Chapter 15, and evaluated in this report. Therefore, the staff finds that the ESF satisfies the requirements of GDC 10 and GDC 20.

The staff conducted a review of the ESF control systems for conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures. The staff concludes that the ESF control systems are testable and are operable using either onsite or offsite power (assuming only one source is available). Additionally, the controls associated with redundant ESF systems are independent and satisfy the single failure criterion and, therefore, meet the relevant requirements of GDC 34, GDC 35, GDC 38, GDC 41, and GDC 44.

In the review of the ESF, the staff examined the dependence of this system on the availability of essential auxiliary systems. Based on this review and coordination with those having primary review responsibility of auxiliary supporting features and other auxiliary features systems, the staff concludes that the design of the ESF is compatible with the functional requirements of auxiliary supporting features and other auxiliary features systems.

The staff reviewed the ITAAC in regards to compliance with 10 CFR 52.47(b)(1). Additional discussion on the staff's review of compliance with 10 CFR 52.47(b)(1) is discussed in Section 14.3.5 of this report. As noted within Section 14.3.5 of this report and this section,

several open items were identified regarding the ITAAC, and upon their satisfactory resolution, the staff finds that the U.S. EPR design meets the requirements of 10 CFR 52.47(b)(1).

## **7.4 Systems Required for Safe Shutdown**

### **7.4.1 Introduction**

To achieve a safe shutdown configuration, the appropriate alignment of systems is required. These systems related to safe shutdown implement the functions associated with attaining and maintaining a safe shutdown condition:

- Reactivity control
- Reactor coolant makeup
- RCS pressure control
- Decay heat removal
- Process monitoring

### **7.4.2 Summary of Application**

**FSAR Tier 1:** The FSAR Tier 1 information associated with this section is found in FSAR Tier 1, Section 2.4, "Instrumentation and Control Systems."

**FSAR Tier 2:** The applicant provided a system description in FSAR Tier 2, Section 7.4, "Systems Required for Safe Shutdown," summarized here, in part, as the following.

ESF systems are used to achieve and maintain safe shutdown. Actuation of ESF systems is performed by the PS. The SAS automatically controls safety-related systems once the systems have been actuated by the PS. The SAS provides grouped command execution, which has been initiated from the SICS. This is designed to provide control of the safety-related systems that are needed to reach safe shutdown of the plant. The HMI is the PICS and SICS. Monitoring and control of the safety-related systems are both available in the MCR and the RSS.

**ITAAC:** The ITAAC associated with safe shutdown systems are given in FSAR Tier 1, Sections 2.4.1, 2.4.2, and 2.4.4.

**Technical Specifications:** The Technical Specifications associated with safe shutdown systems are given in FSAR Tier 2, Chapter 16 (specifically Section 3.3 of the Technical Specifications). The evaluation of the Technical Specifications for the safe shutdown systems is located in Chapter 16 of this report.

### **7.4.3 Regulatory Basis**

The relevant requirements of NRC regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, Section 7.4, "Safe Shutdown Systems," and are summarized below. Review interfaces with other SRP Sections also can be found in NUREG-0800, Section 7.4.

The following requirements apply to FSAR Tier 2, Section 7.4:

1. GDC 1, "Quality Standards and Records," as it relates to assuring structures, systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
2. GDC 2, "Design Bases for Protection Against Natural Phenomena," as it relates to assuring SSCs important to safety shall be designed to withstand the effects of natural phenomena without loss of capability to perform their safety functions.
3. GDC 4, "Environmental and Dynamic Effects Design Bases," as it relates to assuring SSCs important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.
4. GDC 13, "Instrumentation and Control," as it relates to assuring Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.
5. GDC 19, "Control Room," as it relates to providing a control room from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents.
6. GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.
7. GDC 34, "Residual Heat Removal" as it relates to assuring a system to remove residual heat is provided.
8. GDC 35, "Emergency Core Cooling" A system to provide abundant emergency core cooling shall be provided
9. GDC 38, "Containment Heat Removal" as it relates to assuring a system to provide abundant emergency core cooling is provided
10. 10 CFR Part 50, Appendix R, III.G, "Fire Protection of Safe Shutdown Capability"
11. 10 CFR 50.55a(a)(1), "Quality Standards."
12. 10 CFR 50.55a(h), "Protection and Safety Systems," states that IEEE Std 603-1991, including the January 30, 1995, correction sheet, is approved for incorporation by

reference. 10 CFR 50.55a(h)(3), "Safety Systems" requires compliance with IEEE Std 603-1991 and the correction sheet, January 30, 1995.

13. 10 CFR 50.34(f)(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves," or equivalent TMI action plan requirements imposed by Generic Letters.

Acceptance criteria adequate to meet the above requirements include:

SRP Table 7 1, Section 3 (Staff Requirements Memoranda), Section 4 (Regulatory Guides), and Section 5 (Branch Technical Positions), lists the SRP acceptance criteria applicable to systems required for safe shutdown.

#### **7.4.4 Technical Evaluation**

The objective of the staff's review is to confirm that the safe shutdown systems satisfy NRC regulations through a set of acceptance criteria and that they can perform their safety functions for all plant conditions for which they are required.

The U.S. EPR primary Human-Machine Interface is the PICS. Monitoring and control of safety-related systems are both available in the MCR and the RSS. The operator uses the PICS as the primary HMI in the MCR and the RSS to achieve and maintain a safe shutdown condition.

NUREG-0800, Section 7.4, "Safe Shutdown Systems," lists five major design considerations that should be emphasized for the review of safe shutdown systems: (1) Independence; (2) use of digital systems; (3) periodic testing; (4) remote shutdown capability; and (5) safe shutdown. Section 7.1.4.10 of this report addresses independence, and periodic testing is addressed in Section 7.1.4.13 of this report. Remote shutdown capability and safe shutdown are addressed in Sections 7.4.4.2 and 7.4.4.3 of this report.

Several other design considerations are addressed in other Sections of this report, as indicated in Table 7.4 1 below.

**Table 7.4-1 Section 7.4 Design Considerations Referenced in Other Sections of this Report.**

<b>Design Considerations</b>	<b>Report Section(s)</b>
Single-Failure	7.1.4.5
GDC 2, "Design Basis for Protection against Natural Phenomena"	7.1.a.b.c
GDC 4, "Environmental and Missile Design Basis"	7.1.x.y.z
10 CFR 50.55a(a)(3)	7.1.4.1
Testability	7.1.4.21
Control Room, GDC 19, "Control Room"	7.1.4.13, 7.1.4.23
GDC 34, "Residual Heat Removal"	7.3.4.3.11
GDC 35, Emergency Core Cooling"	7.3.4.3.11

Design Considerations	Report Section(s)
GDC 38, "Containment Heat Removal"	7.3.4.3.11
Independence, GDC 21, "Protection System Reliability and Testability"	7.1.4.10
Periodic Testing, GDC 21, "Protection System Reliability and Testability"	7.1.4.13
Divisional Independence	7.1.4.2.2.2
Data Communication	7.1.4.2.3, 7.9.4
Minimum Inventory Requirements for RSS	18.7
Control of Access	7.1.4.15, 7.9.4.3
10 CFR 50.55a(h)(3), GDC 24, "Separation of Protection and Control Systems"	7.1.3.12.3, 7.1.4.12.4
Automatic and Manual Actuation of the SIS	7.3.x.y.z
10 CFR 50.34(f)(xx)	7.5.4.1.1
GDC 1, "Quality Standards and Records," 10 CFR 50.55a(a)(1)	7.1.4.10, 7.1.4.13

10 CFR 50.55a(a)(3) allows applicants under 10 CFR Part 52, to propose alternatives to the requirements of 10 CFR 50.55a(h) or portions thereof. The U.S. EPR design certification applicant proposes to use IEEE Std 603-1998 as an alternative to 10 CFR 50.55a(h)(3) which requires the use of IEEE Std 603-1991. Section 7.1.4.1 of this report discusses the staff evaluation and approval of this alternative.

At the time of the staff's review, the docketed version of the FSAR was Revision 2. However, since FSAR Revision 2, was submitted, the applicant made several changes to the I&C system design and included the details as part of existing FSAR section-related request for additional information (RAI) responses mark-ups. The staff used the provided information in preparing this report. Regarding the information in FSAR Tier 2, Section 7.4, the applicant provided Interim Revision 3 mark-ups for this section in the applicant's March 2, 2011, response to RAI 442, Question 07.09-64. The applicant provided Interim Revision 3 mark-ups for FSAR Tier 2, Section 2.4, in a March 2, 2011, response to RAI 452, Question 07.03-36. Upon receipt of the final Revision 3 of the FSAR, the staff will verify incorporation of the Interim Revision 3 mark-ups. **RAI 452, Question 07.03-36 is being tracked as a confirmatory item.**

#### 7.4.4.1 *Remote Shutdown Capability*

10 CFR Part 50, Appendix A, GDC 13, requires, in part, instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 19 requires, in part, that equipment at appropriate locations outside the control room be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary I&C to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable

procedures. The staff used the guidance in SRP Appendix 7.1 A and SRP Section 7.4 to determine whether the U.S. EPR design meets the requirements of GDC 13 and GDC 19. SRP Section 7.4 identifies review guidance of the RSS that address GDC 13 and GDC 19.

#### *7.4.4.1.1 Operating Independently*

SRP Section 7.4 states that plant designs should provide for control in locations remote from the MCR that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. SRP Section 7.4 also states that remote shutdown equipment should be capable of operating independently of (i.e., without interaction with) the equipment in the MCR. This equipment may include the RSS and other local controls. Additionally, RSS control transfer devices should be located remotely from the MCR and their location should conform to the procedures for remote, alternative, and dedicated shutdown, as appropriate.

FSAR Tier 2, Section 7.4.1.3.4, "Remote Shutdown Station," identifies the RSS as an independent alternative shutdown location that is physically and electrically independent of the MCR, containing necessary equipment to bring the plant to a safe shutdown state during an event requiring evacuation of the MCR. The SICS provides the controls and the PICS provide the displays in the RSS to allow the monitoring and control of the following safe shutdown functions during a fire in the MCR, or during an event that could cause the MCR to become uninhabitable coupled with a single failure:

- Reactivity control
- Reactor coolant makeup
- RCS pressure control
- Decay heat removal
- Control and monitoring of safety support systems for the above functions, as well as essential service water, component cooling water, and onsite power including the emergency diesel generators

During the review, the staff questioned whether SICS provides displays and the necessary manual controls in the RSS. Also, the staff questioned if any SAS manual controls were needed in the RSS. The staff did not identify any ITAAC in FSAR Tier 1, Section 2.4, addressing ESF manual actuations in the RSS. Therefore, in RAI 505 Question 07.04-15, the staff requested that the applicant verify if SICS provides displays in the RSS. **RAI 505 Question 07.04-15 is being tracked as an open item.**

FSAR Tier 2, Section 7.4.1.3.4, states that the MCR-RSS transfer switches maintain divisional independence, so that an electrical failure in one safety division cannot affect another safety division. Divisional independence is discussed in Section 7.1.4.10 of this report. Data communication independence is addressed in Section 7.9.4.5 of this report. FSAR Tier 2, Section 7.4.2.3, "Remote Shutdown Capability," states that the transfer switches will be located in a separate fire zone than the MCR. Additionally, FSAR Tier 1, Section 2.4.2, indicates that the capability to transfer control from the MCR to the RSS exists in a fire area separate from the MCR. The transfer switches are each associated with a single division of the safety-related control and allow transfer of control without entry into the MCR.

10 CFR Part 50, Appendix R, III.G, "Fire Protection of Safe Shutdown Capability," requires, in part, fire protection features be provided for structures, systems, and components important to safe shutdown. SRP Section 9.5.1.1, "Fire Protection Program," provides guidance and acceptance criteria for fire protection programs. This Section states that for operating plants and new design applications, the post fire safe shutdown analysis should describe separation between redundant safe shutdown systems and components.

FSAR Tier 2, Section 9.5.1.1, "Design Basis," states, that an alternative shutdown capability (the RSS), which is physically and electrically independent of the MCR, is used to achieve safe shutdown conditions. FSAR Tier 2, Sections 7.1.1.3.1 and 7.1.1.3.2, describe the capabilities of the SICS and PICS to achieve both hot and cold shutdown conditions from the RSS in case of a fire in the MCR.

In its review, the staff initially found that the applicant did not demonstrate how the requirements of 10 CFR Part 50, Appendix R, III.G, are met. Specifically, FSAR Tier 2, Figure 7.1 5, "Process Information and Control System Architecture" of the FSAR Revision 1, depicts the terminal data network being shared by both the MCR operator workstations and the RSS operator workstations. In addition, the terminal data network is connected to the plant data network through Process Units (PUs). The staff determined that in the event of a fire in the MCR, the applicant had not demonstrated that the terminal data network and the plant data network will not be impacted such that the RSS workstations maintain the capability for hot and cold shutdown to meet the requirements of 10 CFR Part 50, Appendix R, III.G. Therefore, in RAI 309, Question 07.09-60, the staff requested that the applicant address this issue. In a March 5, 2010, response to RAI 309, Question 07.09-60, the applicant stated that PUs and plant data network are physically located in a separate fire area from the MCR and, therefore, unaffected by fire in the MCR. The terminal data network hardware is located so that damage from a fire event in the MCR will be limited to network components required for the operation of MCR workstations and have no impact on the overall functionality of the terminal data network. Portions of the network required for operation from the RSS are located in a separate fire area from the MCR so damage from a fire event in the MCR will be limited to the workstations in the MCR and will not impact the ability to safely shutdown the plant from the PICS workstations in the RSS. The staff finds the applicant's March 5, 2010, response to RAI 309, Question 07.09-60 acceptable. In follow-up RAI 414, Question 07.04-14, the staff requested that the applicant include the information provided in the March 5, 2010, response to RAI 309, Question 07.09-60, in the FSAR. The staff reviewed the applicant's November 29, 2010, response to RAI 414, Question 07.04-14 and also requested that the applicant demonstrate how the various data networks in the main control room (MCR), in the event of a control room fire, would not affect the capability to achieve safe shutdown. The staff reviewed the applicant's March 10, 2010,, response and finds the response satisfactory based on the following:

The March 10, 2010, response to RAI 414, Question 07.04-14 provided an Interim Revision 3 mark-up of FSAR Tier 2, Section 7.1.1.3.2, which included the requested information. Subsequently, on March 28, 2011, the applicant also provided additional applicable Interim Revision 3 mark-ups to FSAR Tier 2, Section 7.1.1.3.2 within a June 22, 1011, response to RAI 442, Question 07.01-26. The information that the staff reviewed in FSAR Tier 2, Section 7.1.1.3.2, Interim Revision 3, March 28, 2011, indicates that the redundant servers and redundant segments of the automation busses are physically located in a separate fire area so that a fire in the MCR does not result in a loss of the PICS in the RSS. Portions of the HMI bus required for operation from the RSS are located in a separate fire area from the MCR, so damage from a fire event in the MCR will be limited to the workstations in the MCR and will not



impact the ability to safely shutdown the plant from the RSS. The staff reviewed this information and finds it acceptable.

The staff finds the RSS meets the requirements in 10 CFR Part 50, Appendix A, GDC 13 and GDC 19, and 10 CFR Part 50, Appendix R, III.G, for independent operation of the RSS and the control transfer switches, once the changes associated with RAI 442, Question 07.01-26 are confirmed. **RAI 442, Question 07.01-26 is being tracked as a confirmatory item.**

#### *7.4.4.1.2 Appropriate Displays and Parameters*

SRP Section 7.4 states that the design of the RSS should provide appropriate displays so that the operator can monitor the status of the shutdown. The design should also maintain parameter indications such that the operators at the MCR and RSS both have access to the same parameters that are being relied upon for safe shutdown.

FSAR Tier 2, Section 18.7.1.3.11, "10 CFR Part 50, Appendix A, GDC 19," indicates that the PICS in the RSS provides the HMI for prompt hot shutdown of the reactor, and also the RSS HMI provides the capability for subsequent cold shutdown. The HMI indicated in FSAR Tier 2, Section 18.7.1.2.2, is the PICS and the SICS. FSAR Tier 2, Section 18.7.4.5, "Remote Shutdown Workstation Alarms, Displays, and Controls," indicates that the RSS minimum inventory includes the readily accessible HMI that the operator needs to perform and confirm a reactor trip and place and maintain the reactor in a safe condition. Section 18.7 of this report provides the staff's evaluation of the minimum inventory requirements for RSS.

FSAR Tier 2, Section 7.4.1.3.4, states that the displays in the MCR and the RSS contain real time plant data prior to, during, and after the control transfer from one station to the other. The RSS data are populated from the same information buses that supply data to the MCR. As such, during the time that control is transferred from the MCR to the RSS or vice versa, data is not lost or interrupted. The RSS contains HMI workstations, with PICS, and select communication equipment, necessary to bring the plant to, and maintain it in a safe shutdown state. The HMI control functions of the RSS are isolated during normal, emergency, routine shutdown, refueling, or maintenance operations as long as the MCR is available. The HMI workstations in the MCR and the RSS will continue to display all parameters available on each workstation while the control functions in the RSS are isolated.

The staff finds that the RSS meets the requirements in 10 CFR Part 50, Appendix A, GDC 13 and GDC 19, for appropriate displays and parameters.

#### *7.4.4.1.3 Accommodating Expected Plant Response*

SRP Section 7.4 states that remote shutdown capability should be capable of accommodating expected plant response following a reactor trip, including protective system actions that could occur as a result of plant cooldown.

FSAR Tier 2, Section 7.4.2.3, states that the RSS contains controls and indications that will allow the operators to control and monitor the safe shutdown systems. Controls and indications of permissive signals are provided in the RSS. The capability to manually validate permissives allows the operator to enable or disable protective functions that may be necessary for proper shutdown of the plant. FSAR Tier 1, Table 2.4.1 7, Items 4.12 and 4.15, provide a means to verify these requirements. Item 4.12 states that a separate set of controls exist on the SICS in the RSS to allow manual validation or inhibition of permissives. FSAR Tier 1, Table 2.4.1 7,

Item 4.15 states that controls exist on the SICS in the RSS that allow manual actuation of reactor trip.

The staff finds that the U.S. EPR RSS design adequately addresses the design requirement for accommodating expected plant responses.

#### *7.4.4.1.4 Control of Access*

SRP Section 7.4 states that access to the RSS should be under strict administrative controls, and use of the control transfer devices should initiate an alarm in the control room. Additional staff discussion on control of access is provided in Sections 7.1.3.15 and 7.9.4.3 of this report.

FSAR Tier 2, Section 7.4.2.3, states that the MCR-RSS transfer switches are key locked, and the keys are maintained by appropriate plant personnel. Alarms in the MCR will alert operators when control is transferred to the RSS. FSAR Tier 2, Section 7.4.1.3.4, indicates that there is an indication on the PICS and SICS showing that RSS control is established. The RSS adequately addresses the requirement in 10 CFR 50.55a(h)(3) for control of access to the RSS. Therefore, the staff finds the RSS control of access acceptable.

#### *7.4.4.2 Safe Shutdown*

The staff used the guidance in SRP Appendix 7.1 A and SRP Section 7.4 to determine whether the U.S. EPR design meets the requirements of GDC 13 and GDC 19.

FSAR Tier 2, Section 7.4.1.1, "I&C Systems Associated with Safe Shutdown," states that ESF are used to achieve and maintain safe shutdown. I&C systems that perform ESF actuation are described in FSAR Tier 2, Section 7.3. The HMI is the PICS and the SICS. The operator uses the PICS as the primary HMI in the MCR and RSS. However, there are some functions that the operator must perform using SICS, which is the credited, safety-related HMI system. FSAR Tier 2, Table 7.1 2, "I&C System Requirements Matrix," identifies the SICS as meeting the requirements of GDC 13 and GDC 19. FSAR Tier 1, Table 2.4.1 9, Item 4.11, provides a means to verify these requirements. FSAR Tier 1, Table 2.4.1 9, Item 4.11 states that controls exist on the SICS in the MCR that allow manual action of the ESF systems at the system level. The staff finds that I&C systems to control safe shutdown are provided by the U.S. EPR design and, therefore, meets the requirements of GDC 13 and GDC 19.

The staff finds the U.S. EPR safe shutdown system adequately addresses the requirements of 10 CFR Part 50, Appendix A, GDC 13, GDC 19, GDC 24, GDC 34, GDC 35, and GDC 38.

### **7.4.5 Combined License Information Items**

No applicable items were identified in the FSAR. No additional COL information items need to be included in FSAR Tier 2, Table 1.8 2, for systems required for safe shutdown consideration.

### **7.4.6 Conclusions**

The staff reviewed the U.S. EPR safe shutdown systems to verify their compliance with applicable regulatory requirements. During the review, the staff reviewed the February 3, 2011, response to RAI 414, Question 07.04-14, which was subsequently superseded by the FSAR Interim Revision 3 mark-ups, submitted with RAI 442, Question 07.01-26. Verification of the final Revision 3 of the FSAR is being tracked as a confirmatory item. When the confirmatory item associated with this RAI is resolved, as well as the confirmatory items associated with

RAI 442, Question 07.09-64, and applicable Sections within Chapter 3, 7, 9, and 18 of the FSAR are finalized to the staff's satisfaction, the staff concludes that the design of the U.S. EPR safe shutdown systems and the safe shutdown initiation of the auxiliary supporting features and other auxiliary features systems are acceptable and meet the relevant requirements of 10 CFR Part 50, Appendix A, GDC 13, and GDC 19.

Appropriate controls are provided for access to the remote shutdown station transfer switches. Therefore, the staff finds the U.S. EPR design meets the requirements of IEEE Std 603-1998, Clause 5.9.

Based on the review, the staff concludes the I&C system maintains variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges during plant shutdown. I&C functions have been provided within the MCR to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including a shutdown following an accident. Equipment at appropriate locations outside the control room provide (1) a design capability for prompt, hot shutdown of the reactor, including necessary I&C to maintain the unit in a safe condition during hot shutdown, and (2) potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. The staff finds the I&C systems required for safe shutdown adequately address the requirements of 10 CFR Part 50, Appendix A, GDCs 13 and 19. Additional staff discussion on the review of 10 CFR Part 50, Appendix A, GDCs 13 and 19, is provided in Sections 7.1.4.3, 7.5.4.2, 7.5.4.3, and 7.6.4.4 of this report.

## **7.5 Information Systems Important to Safety**

### **7.5.1 Introduction**

This section discusses the instrumentation and controls used to provide information important to safety and to provide an indication means for manual operator action for accident mitigation. These include the annunciator systems, accident monitoring instrumentation (AMI), emergency response information capability, and bypass and inoperable status indication.

### **7.5.2 Summary of Application**

FSAR Tier 1: The FSAR Tier 1 information associated with this section is found in FSAR Tier 1, Section 2.4.

FSAR Tier 2: The applicant has provided a system description in FSAR Tier 2, Section 7.5, and summarized as the following.

The information necessary to monitor the nuclear steam supply systems, the containment systems, and the balance of plant is displayed on the operator console and the various screens and panels located within the MCR. Information systems important to safety are those systems that provide information to control and operate the unit safely through all operating conditions, including AOO, accident and post-accident conditions.

ITAAC: The ITAAC associated with FSAR Tier 2, Section 7.5, are given in FSAR Tier 1, Table 2.4.1-7, "Protection System ITAAC," Table 2.4.2 2, "Safety Information and Control System ITAAC," Table 2.4.4-6, "Safety Automation System ITAAC," and Table 2.4.5-3, "Priority and Actuator Control System ITAAC."

Technical Specifications: The Technical Specifications associated with FSAR Tier 2, Section 7.5, are given in FSAR Tier 2, Chapter 16; specifically, U.S. EPR Technical Specifications, Section 3.3.

### **7.5.3 Regulatory Basis**

The relevant NRC regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, Section 7.5, "Information Systems Important to Safety," and are summarized below. Review interfaces with other SRP sections can be found in NUREG-0800, Section 7.5.

Requirements applicable to AMI:

- 1 GDC 1, "Quality Standards and Records," as it relates to assuring structures, systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
- 2 GDC 2, "Design Basis for Protection Against Natural Phenomena"
- 3 GDC 2, "Design Bases for Protection Against Natural Phenomena," as it relates to assuring SSCs important to safety shall be designed to withstand the effects of natural phenomena without loss of capability to perform their safety functions
- 4 GDC 4, "Environmental and Dynamic Effects Design Bases," as it relates to assuring SSCs important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.
- 5 GDC 13, "Instrumentation and Control," as it relates to assuring Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.
- 6 GDC 19, "Control Room," as it relates to providing a control room from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents.
- 7 GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.
- 8 10 CFR 50.55a(a)(1), "Quality Standards."

- 9 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Std 603-1991, and the January 30, 1995, correction sheet. For AMI isolated from the protection system, the applicable requirements of 10 CFR 50.55a(h) for IEEE Std 603-1991 are Clause 5.6.3, "Independence between Safety Systems and Other Systems," and Clause 6.3, "Interaction between the Sense and Command Features and Other Systems."
- 10 10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action plan requirements imposed by orders. The following portions of 10 CFR 50.34(f) applies to AMI:
  - a. 10 CFR 50.34(2)(v), as it relates to bypass and inoperable status indication
  - b. CFR 50.34 (2)(xi), as it relates to direct indication of relief and safety valve position
  - c. CFR 50.34(2)(xii), as it relates to auxiliary feedwater system flow indication (applicable to PWRs only)
  - d. 10 CFR 50.34(2)(xvii), as it relates to AMI
  - e. 10 CFR 50.34(2)(xviii), relates to inadequate core cooling instrumentation
  - f. 10 CFR 50.34(2)(xix), as it relates to instruments for monitoring plant conditions following core damage
  - g. 10 CFR 50.34(2)(xx), as it relates to power for pressurizer level indication
  - h. 10 CFR 50.49(b)(3), "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants"

Requirements applicable to bypassed and inoperable status indication (BISI):

1. GDC 1, "Quality Standards and Records," as it relates to assuring structures, systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
2. GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired 10 CFR 50.55a(a)(1)
3. 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the January 30, 1995, correction sheet. For BISI, the applicable requirements for IEEE Std 603-1991 are Clause 5.8.3, "Indication of Bypasses." For BISI that are isolated from safety systems the requirements for IEEE Std 603-1991 are Clause 5.6.3 and Clause 6.3.
4. 10 CFR 50.34(f)(2)(v) as it relates to bypass and inoperable status indication

Requirements applicable to annunciator systems:

1. GDC 1, "Quality Standards and Records," as it relates to assuring structures, systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
2. GDC 13, "Instrumentation and Control," as it relates to assuring Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.
3. GDC 19, "Control Room," as it relates to providing a control room from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents.
4. GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.
5. 10 CFR 50.55a(a)(1).
6. 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the January 30, 1995, correction sheet. For annunciators that are isolated from the protection system, the applicable requirement(s) of 10 CFR 50.55a(h) for IEEE Std 603-1991 are Clause 5.6.3 and Clause 6.3.

Requirements applicable to the review of safety parameter display system (SPDS), emergency response facility information systems, and emergency response data system (ERDS) information systems:

1. GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired 10 CFR 50.34(f)(2)(iv), SPDS
2. 10 CFR 50.55a(a)(1)
3. 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the January 30, 1995, correction sheet. For SPDS, ERF information systems, and ERDS information

systems isolated from the protection system, the applicable requirements of 10 CFR 50.55a(h) for IEEE Std 603-1991 are Clause 5.6.3, and Clause 6.3.

Acceptance criteria adequate to meet the above requirements include:

The SRP Table 7 1, Section 3 (Staff Requirements Memoranda), Section 4 (Regulatory Guides), and Section 5 (Branch Technical Positions), lists the SRP acceptance criteria applicable to information systems important to safety.

#### **7.5.4 Technical Evaluation**

The objective of the staff's review is to confirm that information systems important to safety satisfy NRC regulations through a set of acceptance criteria and that the information systems important to safety can perform the intended safety functions for all plant conditions.

Information necessary to monitor the nuclear steam supply systems, containment systems, and balance of plant is displayed on the operator console and the various screens and panels located within the MCR. Information systems important to safety are those systems that provide information to control and operate the unit safely through all operating conditions, including AOO, and accident and post accident conditions. However, this report section is limited to the discussion of those display instruments that provide information (1) to enable the operator to assess reactor status, onset and severity of accident conditions, and ESF actuation status and performance, or (2) to enable the operator to reliably perform vital manual actions such as safe shutdown and initiation of manual ESF actuation.

Information systems important to safety are broken down into four subsystems. SRP Section 7.5, Revision 5, lists the following major design considerations that should be emphasized for the review of each system:

##### **Accident Monitoring Instrumentation**

- Conformance to RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," and SRP BTP 7-10, "Guidance on Application of Regulatory Guide 1.97"
- Use of digital systems
- Emergency operating procedures action points
- Monitoring for severe accidents
- Performance assessment

##### **Bypassed or Inoperable Status Indication for Safety Systems**

- Reactor trip system and engineered safety features actuation system
- SRP BTP 7-1, "Guidance on Isolation of Low-Pressure Systems from the High-Pressure RCS"
- SRP BTP 7-2
- SRP BTP 7-6

- Conformance to RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”
- Independence
- Use of digital systems

Plant Annunciator (alarm) Systems

- Reliability
- Use of digital systems
- Independence
- Redundancy

SPDS, Information systems associated with the emergency response facilities (ERF), and Emergency Response Data System

- Independence

Additionally, the SRP lists other criteria that should also be considered. Several of these design considerations are addressed in other sections of this report, as indicated in Table 7.5-1 below

**Table 7.5-1 Design Considerations Referenced in Other Sections of this Report**

Topic	Section(s)
Quality of Components and Modules	7.1.4.7
Independence	7.1.4.10, 7.1.4.12.1, 7.1.4.12.3, 7.9.4.5
Separation of Protection and Control Systems	7.1.4.12.5
SRP BTP 7-1	7.6.4.5
SRP BTP 7-2	7.6.4.5
GDC 1	7.1.4.3
GDC 13 and 19	7.1.4.3, 7.3.4.3.3, 7.4.4.1, 7.4.4.2, 7.6.4.4, Chapter 18
GDC 24	7.1.4.12.3
Automatic and Manual EFW Initiation	7.1.4.28
Setpoint Requirements	7.1.4.26
10 CFR 50.55a(a)(1)	7.1.4.3
SECY-93-087 Item II.T	7.3.4.3.3

10 CFR 50.55a(a)(3) allows applicants under 10 CFR Part 52, to propose alternatives to the requirements of 10 CFR 50.55a(h). The U.S. EPR design certification applicant proposes to use IEEE Std 603-1998 as an alternative to 10 CFR 50.55a(h) which requires the use of IEEE



Std 603-1991, Section 7.1.4.1 of this report discusses the staff evaluation and approval of this alternative.

At the time of the staff's review, the docketed version of the FSAR was Revision 2. However, in response to various RAIs, the applicant provided Interim Revision 3 mark-ups, that the staff used in preparing this report. Regarding the information in FSAR Tier 2, Section 7.5, the applicant provided Interim Revision 3 mark-ups for this section in a May 25, 2011, response to RAI 442 Question 07.01-28. Regarding the information in FSAR Tier 1, Section 2.4.5, the applicant provided Interim Revision 3 mark-ups for this section in a June 22, 2011, response RAI 452, Question 07.03-36. Upon receipt of the final Revision 3 of FSAR, the staff will verify incorporation of the Interim Revision 3 mark-ups. **RAI 452, Question 07.03-36 is being tracked as a confirmatory item.**

#### 7.5.4.1 *Accident Monitoring Instrumentation*

The AMI provides plant process variable information and system status, known as PAM variables, to the operator in the MCR to permit the operator to perform the following:

- Preplanned manual safety functions
- Capability to assess plant conditions, safety system performance, and determine appropriate actions to take to respond to abnormal events
- Capability to bring the plant to a safe shutdown condition

SRP Section 7.5 identifies regulations applicable to AMI. These regulations are addressed below in Sections 7.5.4.1.1 and 7.5.4.1.2 of this report.

##### 7.5.4.1.1 *TMI Related Requirements*

The Three Mile Island (TMI) action plan requirements for I&C systems important to safety are imposed by 10 CFR 50.34(f) for applications pending as of February 16, 1982. 10 CFR Part 52 applicants address the technically relevant portions of the requirements in paragraphs 10 CFR 50.34(f)(1)-(3) except for paragraphs (f)(i)(xii), (f)(2)(ix) and (f)(3)(v). SRP Appendix 7.1-A identifies both the 10 CFR Part 50 and TMI action plan reference numbers for the TMI action plan requirements relevant to Chapter 7. The guidance in SRP Appendix 7.1-A identifies specific acceptance criteria for TMI action plan items.

The following portions of 10 CFR 50.34(f)(2) are applicable to AMI:

- (v) bypass and inoperable status indication
- (xi) direct indication of relief and safety valve position
- (xii) auxiliary feedwater system flow indication
- (xvii) AMI
- (xviii) inadequate core cooling instrumentation
- (xix) monitoring plant conditions following core damage

- (xx) power for pressurizer level indication

The applicant identified that the following TMI action plan items are only applicable to Babcock & Wilcox or boiling water reactor plants and are not applicable to the U.S. EPR design:

- Failure Modes and Effects Analysis of Integrated Control System
- Anticipatory Trip on Loss of Main Feedwater or Turbine Trip
- Central Reactor Vessel Water Level Recording

The staff agrees with the applicant's determination. The TMI action plan items applicable to the U.S. EPR design are discussed in the subsections that follow.

10 CFR 50.34(f)(2)(v) requires an automatic indication of the bypassed and inoperable status of safety systems. FSAR Tier 2, Section 7.5.2.1.1, "10 CFR 50.34(f), 'Additional TMI Related Requirements'," indicates that if any PAM Type A, B, and C variable is bypassed or rendered inoperable, an indication is provided to the operator in the MCR. According to FSAR Tier 2, Section 7.5.1.4, "Bypass and Inoperable Status Indication," BSI of safety-related systems is provided by the PICS. According to FSAR Tier 2, Section 7.5.2.2.4, "Conformance to Regulatory Guide 1.47," if either the PS or the SAS is bypassed or inoperable, an automatic output is provided to the PICS. Additional staff discussion is provided below in Section 7.5.4.2 of this report.

10 CFR 50.34(f)(2)(xi) requires a direct indication of relief and safety valve position (open or closed) in the MCR. FSAR Tier 2, Section 7.5.2.1.1, states that each of the three PSRVs is provided with a position sensor. The position (open or closed) for each valve is indicated in the MCR.

10 CFR 50.34(f)(2)(xii) requires automatic and manual auxiliary feedwater system initiation and flow indication in the main control room. Section 7.1.4.28 of this report discusses automatic and manual EFW initiation. FSAR Tier 2, Section 7.5.2.1.1, states that indication of EFW flow to each SG is provided in the MCR. FSAR Tier 2, Section 10.4.9.3, "Safety Evaluation," states the EFW system automatically initiates upon system actuation signal and has the capability of manual initiation of protective actions.

10 CFR 50.34(f)(2)(xvii) requires instrumentation to measure, record, and readout in the MCR: (1) Containment pressure; (2) containment water level; (3) containment hydrogen concentration; (4) containment radiation intensity (high level); and (5) noble gas effluents at all potential, accident release points. FSAR Tier 2, Section 7.5.2.1.1, states the following instrumentation is available for readout in the MCR:

- Containment pressure sensors are provided by the containment ventilation system.
- Level sensors for the in containment refueling water storage tank are provided by the SIS.
- Containment hydrogen sensors are provided by the hydrogen monitoring system
- Containment radiation intensity (high level) monitors are provided by the radiation monitoring system

- Noble gas effluent monitoring at all potential accident release points is provided by the RMS
- Continuous sampling of radio-iodine and particulates from accident release points

10 CFR 50.34(f)(2)(xviii) requires that instruments in the control room provide unambiguous indication of inadequate core cooling. FSAR Tier 2, Section 7.5.2.1.1, states the following instrumentation provides an indication in the MCR of inadequate core cooling:

- The reactor vessel water level indication is provided by the reactor pressure vessel water level measurement system described in FSAR Tier 2, Section 7.1.1.5.7, "Reactor Pressure Vessel Level Measurement System."
- A combination of RCS hot leg wide range pressure and the core outlet thermocouples as described in FSAR Tier 2, Section 7.1.1.5.2, "Incore Instrumentation System," is used to determine inadequate core cooling.

10 CFR 50.34(f)(2)(xix) requires instrumentation adequate for monitoring plant conditions following an accident that includes core damage. Instrumentation used during severe accident conditions are identified in FSAR Tier 2, Table 19.2 3, "Severe Accident Instrumentation and Equipment." The instrumentation is designed so there is reasonable assurance that the instrumentation will operate in the severe accident environment for which they are intended and over the time span for which they are needed. FSAR Tier 2, Section 19.2.3.3.7, "Equipment Survivability," discusses equipment survivability during severe accidents. FSAR Tier 2, Section 7.5.2.1.2, "GDC 13, 'Instrumentation and Control'," identifies the PICS and SICS as providing capability for monitoring variables, including PAM variables and system variables over their anticipated ranges for normal operation, for AOO, and for accident conditions as appropriate. This monitoring provides reasonable assurance of safety by including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, or the containment and its associated systems. FSAR Tier 2, Section 7.5.2.2.1, "Conformance with Regulatory Guide 1.97 and BTP 7-10," states that the I&C systems that perform the AMI functions are designed in accordance with the criteria of IEEE Std 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," with modifications specified in RG 1.97, Revision 4, and in accordance with the supplemental guidance provided in SRP BTP 7-10. ITAAC regarding the PAM instrumentation is provided in FSAR Tier 1, Table 3.7 2, "Accident Monitoring Instrumentation ITAAC." The staff review and discussion on ITAAC for the PAM is also addressed in Section 14.3.5 of this report.

10 CFR 50.34(f)(2)(xx) requires power supplies for pressurizer relief valves, block valves, and level indicators such that:

- Level indicators are powered from vital buses.
- Motive and control power connections to the emergency power sources are through devices qualified in accordance with requirements applicable to systems important to safety.
- Electric power is provided from emergency power sources.

FSAR Tier 2, Section 7.5.2.1.1, states:

Each of the four PZR [pressurizer] level sensors generates a signal that is received in one of the four divisions of the PS. The PZR level sensors are powered from the Class 1E bus of the PS division in which the sensor signal is received. PZR level indication is provided by both the PICS and the safety related SICS.

Each division of the PS and the SICS is supplied by an independent Class 1E, uninterruptible electrical bus. These busses are backed by the emergency diesel generators to cope with loss of offsite power. Inside a division, the PS cabinets are supplied by two redundant, uninterruptible 24 Vdc. To cope with loss of onsite and offsite power, the feeds to the PS cabinets are supplied with two hour batteries.

Equipment qualification of power connections to emergency power sources is discussed in Section 3.11 of this report.

Based on the review of the design requirements provided in FSAR Tier 2, the staff finds the AMI system adequately addresses the applicable requirements of 10 CFR 50.34(f)(2).

#### *7.5.4.1.2 Post-Accident Monitoring Instrumentation*

GDC 13, and GDC 19 address AMI. GDC 13 requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 19 requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss of coolant accidents. To assess the AMI design against the regulations, the staff used the guidance found in SRP Appendix 7.1 A, SRP Section 7.5, RG 1.97, Revision 4, RG 1.105, and SRP BTP 7-10.

FSAR Tier 2, Section 7.5.2.1.2, identifies the PICS and SICS as providing capability for monitoring variables, including PAM variables and system variables over their anticipated ranges for normal operation, for AOO, and for accident conditions as appropriate. This monitoring provides reasonable assurance of safety by including those variables and systems that can affect the fission process, integrity of the reactor core, reactor coolant pressure boundary, or containment and its associated systems. FSAR Tier 2, Section 7.5.1.2, "Post-Accident Monitoring Instrumentation," states that the AMI provides plant process variable information and system status, known as PAM variables, to the operator in the MCR to permit the operator to perform the following:

- Preplanned manual safety functions
- Capability to assess plant conditions, safety system performance, and determine appropriate actions to take to respond to abnormal events
- Capability to bring the plant to a safe shutdown condition

The primary operator interface for displaying PAM variables is the non-safety-related PICS. Additionally, Types A through C PAM variables are displayed on the safety-related SICS. Additional discussion on PICS, as the preferred operator interface, is located in

Sections 7.1.4.2.2.1 and 7.1.4.14 of this report. As the safety-related user interface, SICS is designed to meet the requirements of GDC 13 and GDC 19. FSAR Tier 2, Section 7.5.2.2.1 states that the I&C systems that perform the AMI functions are designed in accordance with the criteria of IEEE Std 497-2002 with modifications specified in RG 1.97, Revision 4, and in accordance with the supplemental guidance provided in SRP BTP 7-10. RG 1.97, Revision 4, indicates that the AMI and PAM variables should be selected based on emergency guidelines and procedures. IEEE Std 497-2002 provides performance based criteria for selecting variables and recommends determining the variable type according to its accident management function. The accident management function is to be identified by its use in the Emergency Procedure Guidelines, Emergency Operating Procedures, and Abnormal Operating Procedures. The development of these guidelines and procedures is discussed in FSAR Tier 2, Section 13.5, "Plant Procedures." IEEE Std 497-2002, Clause 5.6 requires documentation of the assessment for each performance criteria: range, accuracy, response time, required instrument duration, and reliability. The assessment is performed to assure the as designed performance meets or exceeds the performance criteria. FSAR Tier 2, Section 7.5.2.2.1 discusses the performance assessment. For each of the performance criteria, results shall be documented and a graded approach to develop setpoints will be used based on their importance to safety. SRP Section 7.5 identifies RG 1.105 as providing acceptable guidance in establishing measurement uncertainties. RG 1.105 endorses ISA S67.04-1994, "Setpoints for Nuclear Safety Related Instrumentation." Furthermore, by conforming to RG 1.97, Revision 4, certain PAM equipment will meet environmental and seismic qualification per 10 CFR 50.49(b)(3). IEEE Std 497-2002, Clause 7 presents the environmental and seismic qualification criteria of Type A, B, C, D, and E variables. The staff review and discussion of how the U.S. EPR design addresses setpoint requirements is located in Section 7.1.4.26 of this report. The staff review and discussion of how the U.S. EPR design addresses equipment qualification is located in Section 3.11 of this report.

As indicated in the paragraph above, RG 1.97, Revision 4, indicates that the AMI and PAM variables should be selected based on emergency guidelines and procedures. The list of accident monitoring variables is provided in FSAR Tier 2, Table 7.5 1, "Initial Inventory of Post Accident Monitoring Variables," and will be confirmed by the COL applicant prior to fuel load. ITAAC is provided in FSAR Tier 1, Table 3.7 2, Items 2.1, 3.1, 3.2, 3.3, and 3.4. While the design description in FSAR Tier 1 and FSAR Tier 2 appear sufficiently complete to meet the requirements of GDC 13, the current design descriptions suggest otherwise. Specifically, current design descriptions imply the PAM inventory is "initial" and further work is needed to complete the PAM inventory. Furthermore, the associated PAM ITAAC should ensure that the PAM variables are verified once the emergency operating procedures have been developed. As part of the May 25, 2011, response to RAI 442, Question 07.01-28, the applicant provided FSAR Tier 2, Section 7.5, Revision 3-Interim. During a public meeting, the staff and the applicant discussed the information in FSAR Tier 2, Section 7.5, Interim Revision 3 mark-ups. The applicant stated that it would revise the title of FSAR Tier 2, Table 7.5-1, to "Inventory of Post-Accident Monitoring Variables." Additionally, the applicant stated that it would revise the wording in FSAR Tier 2, Section 7.5.2.2.1, to state that the inventory list of accident monitoring variables in FSAR Tier 2, Table 7.5-1 would be verified. Furthermore, the applicant stated that it would revise the wording in ITAAC Item 2.1 to be consistent with FSAR Tier 2. The purpose of the revisions was to demonstrate that the U.S. EPR design was sufficiently complete to support design certification, as discussed in 10 CFR 52.47. Therefore, in RAI 505, Question 07.05-10, the staff requested that the applicant address the associated changes regarding completeness of the PAM variables. **RAI 505, Question 07.05-10 is being tracked as an open item.**

#### 7.5.4.2 *Bypassed and Inoperable Status Indication*

Bypassed and inoperable status indication of safety-related systems is provided by the PICS. SRP Section 7.5 identifies the regulations as applicable to BISI.

As discussed in the above Section 7.5.4.1.1 of this report, 10 CFR 50.34(f)(2)(v) requires an automatic indication of the bypassed and inoperable status of safety systems. IEEE Std 603-1998, Clause 5.8.3, requires indication of bypasses. For review of how bypass and inoperable status indication meets the regulation, the staff used SRP Section 7.5 and RG 1.47. Additionally, bypassed and inoperable status of electrical auxiliary support features are described in Section 8.3 of this report.

FSAR Tier 2, Section 7.5.2.1.1, indicates that if any PAM Type A, B, and C variable is bypassed or rendered inoperable, an indication is provided to the operator in the MCR. The BISI is provided by the PS and the SAS and is displayed by the PICS. From FSAR Tier 2, Section 7.5.2.2.4, if either the PS or the SAS is bypassed or inoperable, an automatic output is provided to the PICS. FSAR Tier 2, Section 7.5.2.2.5, "Scope of Bypassed and Inoperable Status Indications," describes the scope of BISI to include reactor trip functions, ESF functions, safety injection system accumulator isolation valves, and residual heat removal system suction isolation valves. Based on the description specified in FSAR Tier 2, Section 7.5.2.2.5, the staff finds the BISI adequately addresses the requirements of 10 CFR 50.34(f)(2)(v) and IEEE Std 603-1998, Clause 5.8.3.

#### 7.5.4.3 *Annunciator Systems*

SRP Section 7.5 identifies applicable regulations for annunciator systems. 10 CFR Part 50, Appendix A, GDC 13, requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, anticipated operational occurrences, and accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, integrity of the reactor core, reactor coolant pressure boundary, and containment and its associated systems. 10 CFR Part 50, Appendix A, GDC 19, requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss of coolant accidents. The staff used the guidance in SRP Appendix 7.1 A, SRP Section 7.5, and RG 1.97. to assess how the U.S. EPR annunciator system design meets the requirements of GDC 13 and GDC 19.

FSAR Tier 2, Section 7.5.2.2.6, "Redundancy and Diversity of Display," describes the redundancy and diversity of the alarms. Type A, B, and C accident monitoring variables are sent directly from the SCDS to the SICS via hardwired connections bypassing software based components. Diverse display of variables is not required. The same variables are processed through the PAS and PICS to provide a redundant path. The staff review and discussion of the SCDS is addressed in Section 7.1 of this report. FSAR Tier 2, Section 7.1.2.3.2, "SRM to SECY-93 087, Item II.T – Control Room Annunciator (Alarm) Reliability," states conformance to the SRM to SECY 93 087, Item II.T is provided by redundant processing units for transmittal of alarms to the operator workstations and hardwired SICS panels in the MCR, and multiple workstations in the MCR in which each workstation has the same capabilities with regards to monitoring and control of plant systems. Conformance to SRM to SECY 93 087, Item II.T, which indicates that alarms for specific manual control for which no automatic control is provided, are to meet Class IE requirements, is satisfied by the accident monitoring provided by the safety-related SICS.

FSAR Tier 2, Section 7.5.1.1, "Annunciator Systems," states the annunciator system consists of alarms and functions to enable operators to silence, acknowledge, reset, and test alarms. The PICS is the primary annunciator system, with the SICS providing limited backup functions to support accident mitigation. The SICS is the credited, safety-related system that is required to meet GDC 13 and GDC 19. FSAR Tier 2, Section 7.5.1.1, "Annunciator Systems," indicates that the minimum inventory of MCR alarms, displays, and controls that are readily accessible to the operator is credited for EOP actions to bring the plant to a safe condition or to carry out risk-important operator actions. The staff finds the U.S. EPR annunciator system adequately addresses the requirements of GDC 13 and GDC 19.

#### 7.5.4.4 *Emergency Response Information*

SRP Section 7.5 identifies applicable regulations for the Safety Parameter Display System and for information system associated with the Emergency Response Data System; 10 CFR 50.55a(a)(1), GDC 1, and GDC 24.

FSAR Tier 2, Section 18.7.1.3.3, "10 CFR 50.34(f)(2)(iv)-Safety parameter Display System," Revision 2, indicates that the human system interface (HSI) meets the requirements for a SPDS, and that the parameters required to be displayed as part of the safety parameter display system are made available on the PICS and the SICS in the MCR, the technical support center.

FSAR Tier 2, Section 7.5.1.3, "Emergency Response Information," Interim Revision 3, indicates that the SPDS, ERDS and TSC are designed and implemented in accordance with NUREG-0696, "Functional Criteria for Emergency Response Facility, NUREG-0654, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," and NUREG-0737, "Clarification of TMI Action Plan Requirements." The PICS provides the safety parameter display system display. The applicant identified the guidelines to which the safety parameter display system and for information system associated with the emergency response data system conform. Additionally, the non-safety portions of the information systems important to safety are isolated from the safety systems. The staff's review of PICS and SICS compliance to 10 CFR 50.55a(a)(1), GDC 1, and GDC 24 is found in Sections 7.1.4.3 and 7.1.4.10 of this report.

#### 7.5.5 **Combined License Information Items**

No applicable items were identified in the FSAR. However, the staff noted that the reference combine license plant possessed a combined license information item regarding the update of PAMS variables. Therefore, in RAI 505, Question 07.05-11, the staff requested that the applicant address the need for that combined license information item. Also, the staff did not see any combined license information items for PAMS instruments that are likely to be site-specific. Therefore, the staff also requested that the applicant identify any site-specific instrumentation that may need to be a combined license information item. To address these issues, **RAI 505, Question 07.05-11 is being tracked as an open item.**

#### **Conclusions**

The staff reviewed the U.S. EPR information systems important to safety to verify compliance with applicable regulations. When the applicable sections within Chapters 7, 14, and 18 of the FSAR are finalized to the staff's satisfaction, and except for the open and confirmatory items identified herein, the staff concludes that the design of the U.S. EPR information systems

important to safety should be acceptable to meet the relevant requirements of 10 CFR 50.34(f), 10 CFR 50.55a(h), and 10 CFR Part 50, Appendix A, GDC 1, GDC 13, and GDC 19.

The AMI includes the following functions required by 10 CFR 50.34(f)(2): Auxiliary feedwater system flow indication; AMI; inadequate core cooling instrumentation; and instruments for monitoring plant conditions following core damage. Additionally, the power supply for the AMI pressurizer level indication complies with the requirements of 10 CFR 50.34(f)(2)(xx). Therefore, the staff concludes that the instrumentation systems important to safety satisfy the applicable requirements of 10 CFR 50.34(f)(2), Subparts xi, xii, xvii, xviii, xix, and xx.

The staff reviewed the systems for which a bypassed or inoperable status is indicated in the control room. The staff finds that the bypass indications will give the operators timely information and status reports so the operators can mitigate the effects of unexpected system unavailability. The bypass indications satisfy the guidelines of RG 1.47. Therefore, the staff concludes that the BISI functions satisfy the applicable requirements of 10 CFR 50.55a(h) and 10 CFR 50.34(f)(2)(v).

The staff reviewed the control room annunciator systems and determined that these systems are sufficiently reliable to support normal and emergency plant operations. Redundant annunciator systems are provided by SICS and PICS and are independent, thus meeting independence requirements of IEEE Std 603-1998, Clause 5.6. Alarms provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions comply with the criteria of IEEE Std 603-1998. Therefore, the staff concludes that the annunciator systems satisfy the guidance of the SRM on SECY-93 087 Item II.T, and meet the requirements of 10 CFR Part 50, Appendix A, GDC 13 and GDC 19.

## **7.6 Interlock Systems Important to Safety**

### **7.6.1 Introduction**

The interlock functions important to safety reduce the probability of occurrence of specific events or maintain safety systems in a state that provides reasonable assurance of their availability.

### **7.6.2 Summary of Application**

**FSAR Tier 1:** FSAR Tier 1 information associated with this Section is found in FSAR Tier 1, Section 2.2.3, "Safety Injection System and Residual Heat Removal System," Section 2.2.6, "Chemical and Volume Control System," Section 2.4, "Instrumentation and Control Systems," Section 2.4.1, "Protection System," Section 2.4.2, "Safety Information and Control System," Section 2.4.4, "Safety Automation System," Section 2.4.5, "Priority and Actuator Control System," and Section 2.4.10, "Process Information and Control System."

**FSAR Tier 2:** The applicant provided a system description in FSAR Tier 2, Section 7.6, "Interlock Systems Important to Safety," and summarized in the following discussion.

The control logic for the interlock functions important to safety is processed by the PS, with the exception of the interlocks to maintain separation between redundant component cooling water system (CCWS) trains. The control logic for the CCWS interlocks is processed by the SAS.



When plant conditions dictate that an interlock be activated, the interlock signal is sent from the PS or SAS to the PACS. While the interlock signal is present, the PACS will prevent an override of the interlock by actuation or control orders having a lower priority than the interlock function. When plant conditions are such that an interlock can be removed, the PS or SAS removes the interlock signal, and the PACS allows the actuator to be influenced by other control systems.

The capability to perform manual actions related to these interlocks (i.e., acknowledgement of permissive signal status) is provided on the SICS.

**ITAAC:** The ITAAC associated with FSAR Tier 1, Section 2.2.3 are given in Table 2.2.3 3, "Safety Injection System and Residual Heat Removal System ITAAC," Section 2.2.6 are given in Table 2.2.6 3, "Chemical and Volume Control System ITAAC," Section 2.4 are given in Table 2.4.1-7, "Protection System ITAAC," Table 2.4.2 2, "Safety Information and Control System ITAAC," Table 2.4.4 6, "Safety Automation System ITAAC," Table 2.4.5 3, "Priority and Actuator Control System ITAAC," and Table 2.4.10 1, "Process Information and Control System ITAAC." The evaluation of the ITAAC associated with Interlock Systems Important to Safety is discussed in Section 14.3.5 of this report.

**Technical Specifications:** The Technical Specifications associated with FSAR Tier 2, Section 7.6, are given in FSAR Tier 2, Chapter 16; specifically Sections 3.3 and B3.3 of the U.S. EPR Technical Specifications and Technical Specifications Bases, respectively. The evaluation of the Technical Specifications associated with Interlock Systems Important to Safety is discussed in Chapter 16 of this report.

### 7.6.3 Regulatory Basis

The relevant NRC regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, Section 7.6. "Interlock Systems Important to Safety," and summarized below. Review interfaces with other SRP Sections also can be found in NUREG-0800, Section 7.6.

- 1 GDC 1, "Quality Standards and Records," as it relates to assuring structures, systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
- 2 GDC 2, "Design Bases for Protection Against Natural Phenomena," as it relates to assuring SSCs important to safety shall be designed to withstand the effects of natural phenomena without loss of capability to perform their safety functions.
- 3 GDC 4, "Environmental and Dynamic Effects Design Bases," as it relates to assuring SSCs important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.
- 4 GDC 13, "Instrumentation and Control," as it relates to assuring Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.

- 5 GDC 19, "Control Room," as it relates to providing a control room from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents.
- 6 GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.
- 7 10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements, Bypass and Inoperable Status Indication," or equivalent TMI action requirements imposed by Generic Letters

Additional requirements applicable to safety systems with which interlock systems may interact are provided below.

1. GDC 10, "Reactor Design" as it relates to the reactor core and associated coolant, control, and protection systems to assure that specified acceptable fuel design limits are not exceeded during any conditions.
2. GDC 15, "RCS (RCS) Design," to ensure the reactor coolant system and associated auxiliary, control, and protection systems design has sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition.
3. GDC 16, "Containment Design" as it relates to assuring that a reactor containment and associated systems are provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded.
4. GDC 28, "Reactivity Limits" as it relates to assuring that reactivity control systems are designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly the capability to cool the core.
5. GDC 33, "Reactor Coolant Makeup," as it relates assuring a system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary.
6. GDC 34, "Residual Heat Removal," as it relates to assuring a system to remove residual heat is provided.
7. GDC 35, "Emergency Core Cooling," A system to provide abundant emergency core cooling shall be provided

8. GDC 38, "Containment Heat Removal," as it relates to assuring a system to provide abundant emergency core cooling is provided
9. GDC 41, "Containment Atmosphere Cleanup," as it relates to assuring Systems to control fission products, hydrogen, oxygen, and other substances which may be released into the reactor containment are provided
10. GDC 44, "Cooling Water," as it relates to assuring that a system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink is provided.
11. 10 CFR 50.55a(a)(1), "Quality Standards"
12. 10 CFR 50.55a(h), "Protection and Safety Systems," states that IEEE Std 603-1991, including the January 30, 1995, correction sheet is approved for incorporation by reference. 10 CFR 50.55a(h)(3), "Safety Systems," requires compliance with IEEE Std 603-1991 and the January 30, 1995, correction sheet.

Additionally, SRP Table 7 1, Section 2, identifies GDC 25, "Protection System Requirements for Reactivity Control Malfunctions," for FSAR Tier 2, Section 7.6.

Acceptance criteria adequate to meet the above requirements include:

SRP Table 7 1, Section 3 (Staff Requirements Memoranda), Section 4 (Regulatory Guides), and Section 5 (Branch Technical Positions), lists the SRP acceptance criteria applicable to interlock systems important to safety.

#### **7.6.4 Technical Evaluation**

The objective of the staff's review is to confirm that the interlock systems important to safety satisfy NRC regulations through a set of acceptance criteria and that the interlock systems can perform their safety functions for all plant conditions.

SRP Section 7.6 lists the following major design considerations that should be emphasized for the review of interlock systems important to safety:

- Single failure criterion
- Quality of components and modules
- Independence
- System testing and inoperable surveillance
- Use of digital systems
- Interlocks to prevent over-pressurization of low pressure systems
- Interlocks to prevent over pressurization of the primary coolant during low temperature operations of the reactor vessel
- Interlocks for emergency core cooling system accumulator valves

- Interlocks required to isolate safety systems from non safety systems
- Interlocks required to preclude inadvertent inter ties between redundant or diverse safety systems

Several of these design considerations are addressed in other sections of this report, as indicated in Table 7.6 1 below. The remaining major design considerations are discussed below. Additionally, the SRP lists other requirements applicable to interlock systems, including instrumentation and control available to operators, control room design, and bypass and inoperable status indication, which are addressed below.

**Table 7.6-1 Section 7.6 References to Other Report Sections.**

<b>Design Consideration</b>	<b>Report Section(s)</b>
Quality of Components and Modules	7.1.4.7
Single Failure	7.1.4.5
Independence	7.1.4.10, 7.1.4.12.1, 7.1.4.12.3, 7.9.4, 7.9.4.5
Control Room	7.1.4.14, 7.1.4.23, 7.1.4.2.28, 7.4.4.1, 7.4.4.2
Clause 5.6	7.1.4.10
Clause 5.6.1	7.1.4.10.1, 7.9.4.5
Clause 5.6.2	7.1.4.12.2
Clause 5.6.3	7.1.4.12.3, 7.9.4.5
Clause 5.6.3.1	7.1.4.12.4
Clause 5.6.3.2	7.1.4.12.5
Clause 5.6.3.3	7.1.4.12.6
SCDS	7.1.x.y.z
GDC 13 and GDC 19	7.1.4.3, 7.4.4.1, 7.4.4.2, 7.5.4.1.2, and 7.5.4.3
Bypass and Inoperable Status Indication	7.5.4.2
Interlock Systems Quality, Use of Digital Systems, and Reliability	7.1.4.21
Qualification Programs	3.10, 3.11
GDC 1, GDC 2, GDC 4, GDC 15, GDC 16, GDC 28, GDC 33, GDC 34, GDC 35, GDC 38, GDC 41, GDC 44, 10 CFR 50.55a(a)(1)	7.1

10 CFR 50.55a(a)(3) allows an applicant under 10 CFR Part 52, to propose alternatives to the requirements of 10 CFR 50.55a(h)(3) or portions thereof. The U.S. EPR design certification applicant proposes to use IEEE Std 603-1998, as an alternative to 10 CFR 50.55a(h)(3) which requires the use IEEE Std 603-1991. Section 7.1.4.1 of this report discusses the staff evaluation and approval of this alternative.

At the time of the staff's review, the docketed version of the FSAR was Revision 2. However, since FSAR Revision 2, was submitted, the applicant made several changes to the I&C system design and included the details as part of existing FSAR section-related request for additional information (RAI) response mark-ups. The staff used the provided information in preparing this report. Regarding the information in FSAR Tier 2, Section 7.6, the applicant provided Interim Revision 3 mark-ups for this section in a May 20, 2011, response to RAI 442, Question 07.09-64. The applicant provided FSAR Tier 1, Section 2.4, Interim Revision 3 mark-ups, in a June 22, 2011, response to RAI 452, Question 07.03-36. Upon receipt of the final Revision 3 of the FSAR, the staff will verify incorporation of the Interim Revision 3 mark-ups. **RAI 452, Question 07.03-36 is being tracked as a confirmatory item.**

#### 7.6.4.1 *Single Failure Criterion*

IEEE Std 603-1998, Clause 5.1, "Single Failure Criterion," requires that a safety system shall perform all safety functions required for a design basis event in the presence of:

- any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures
- all failures caused by the single failure
- all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions

The staff used the guidance in SRP Section 7.6 and SRP Appendix 7.1 C to determine how the U.S. EPR design may comply with IEEE Std 603-1998, Clause 5.1.

FSAR Tier 2, Section 7.6.1.2, "Functional Descriptions," provides a functional description of the interlocks. For residual heat removal (RHR) suction valve interlocks, safety injection accumulator interlocks, and interlocks to provide low temperature over pressure protection (LTOP), single failure criterion is met by having actuation logic units within redundant PS divisions, each sending the interlock signal to its respective isolation valves in each of two trains. For example, PS division one holds closed a single RHR suction valve in train one and a single RHR suction valve in train two. PS division two holds closed a single RHR suction valve in train two and a single RHR suction valve in train one. Interlocks isolating redundant CCWS trains meet the single failure criterion by having each redundant SAS division control its respective CCWS train isolation valves. Also, each valve is equipped with redundant open closed position sensors preventing inadvertent connection of redundant CCWS trains. Additional discussion on CCWS train isolation from the system layout and mechanical perspective is provided in Section 9.2 of this report. The staff finds the U.S. EPR interlock systems important to safety adequately address the requirements of IEEE Std 603-1998, Clause 5.1. System level accommodation of single failures for the PS, SAS, and PACS is addressed in Section 7.1.4.5 of this report.

#### 7.6.4.2 *Independence*

IEEE Std 603-1998, Clause 5.6, requires physical, electrical, and communication independence between redundant portions of safety systems, safety systems and the effects of design basis events, and safety systems and other systems. Table 7.6 1, "References to Other Sections of the Report," of this report indicates the report sections that provide the discussion of the staff review addressing IEEE Std 603-1998, Clauses 5.6, 5.6.1, 5.6.2, 5.6.3, 5.6.3.1, 5.6.3.2,

and 5.6.3.3. The guidance of SRP Appendix 7.1 C indicates that in regard to IEEE Std 603-1998, Clause 6.3, the staff reviews the application to confirm that the applicant's non-safety system interactions with safety systems are limited, such that the requirements of 10 CFR Part 50, Appendix A, GDC 24, are met. GDC 24 requires, in part, that the protection system shall be separated from control systems to the extent that failure of any single control system component, or channel, which is common to the control and protection systems, leaves intact a system satisfying all requirements of the protection system. To determine whether the U.S. EPR design complies with IEEE Std 603-1998, Clauses 5.6 and 6.3, the staff referenced the guidance found in SRP Section 7.6 and SRP Appendix 7.1 C. SRP Appendix 7.1 C indicates that when the event of concern is failure of a sensing channel shared between control and protection functions, an acceptable approach is to isolate the safety system from channel failure and isolate the control system from channel failure.

FSAR Tier 2, Section 7.6.2.1.3, "Compliance to Requirements for Independence (Clauses 5.6 and 6.3 of IEEE Std 603 1998)," states that redundant divisions of the safety-related I&C systems are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing their function. I&C equipment required to perform the interlock functions is independent from the effects of design basis events. The PS and SAS do not rely on input from non-safety-related systems to perform the interlock functions. Certain sensor measurements are used as inputs to both a safety-related interlock function and a non-safety-related control function performed by a non-safety-related I&C system. In these cases, the signal conditioning and distribution system is provided to condition and distribute signal inputs needed within multiple distributed control systems. The staff review and discussion of the SCDS is addressed in Section 7.1 of this report.

By having redundant and independent divisions of the safety-related I&C systems, and both electrical and communications independence as described in Section 7.1.4.10 of this report, the staff finds the U.S. EPR interlock systems important to safety adequately address the requirements of IEEE Std 603-1998, Clause 5.6. Sensor information from safety-related systems passes through electrically isolated connections to non safety-related systems. The staff finds the U.S. EPR interlock systems important to safety adequately address the requirements of IEEE Std 603-1998, Clause 5.6, 6.3, and GDC 24. System independence is also discussed in Sections 7.1.4.10, of this report.

#### 7.6.4.3 *System Testing and Inoperable Surveillance*

IEEE Std 603-1998, Clause 5.7, requires capability for test and calibration of safety system equipment, while retaining capability of the safety systems to accomplish their safety functions. IEEE Std 603-1998, Clause 5.8 requires information displays for manually controlled actions, system status indication, indication of bypasses, and accessibility to the operator. IEEE Std 603-1998, Clause 6.5 requires capability for test and calibration of sense and command equipment. 10 CFR 50.34(f)(2)(v) requires an automatic indication of the bypassed and inoperable status of safety systems. To determine whether the U.S. EPR design meets IEEE Std 603-1998, Clauses 5.7, 5.8, 6.5, and 10 CFR 50.34(f)(2)(v), the staff relied on the guidance found in SRP Section 7.6 and SRP Appendix 7.1 C.

FSAR Tier 2, Section 7.6.2.1.4, "Compliance to Requirements for System Testing and Inoperable Surveillance," discusses system testing and inoperable surveillance. Surveillance is accomplished through overlapping tests to verify performance of the interlock function from sensor to PACS module. Periodic testing of sensors and acquisition circuits can be performed while maintaining the interlock function in its current state. Self testing is performed during

power operations with extended self testing performed during outages to verify functionality that cannot be tested with the reactor at power. For connections between the output circuits of the PS, SAS, and the PACS modules, to the actuators, surveillance of interlocking functions during power operations can be satisfied by observing the interlocked position of the actuators. Safety-related I&C systems are designed to provide bypass and inoperable status information to the operator. Sufficient indications are provided to the operator to evaluate the status of each interlock as described in FSAR Tier 2, Section 7.6.1.2.

By having periodic manual testing while maintaining interlock functions and having automatic self testing performed both at power and during outages, the staff finds the U.S. EPR interlock systems important to safety adequately address the requirements of IEEE Std 603-1998, Clauses 5.7 and 6.5. The safety-related I&C systems provide bypass and inoperable status information, as well as indications to evaluate the status of each interlock, thus satisfying IEEE Std 603-1998, Clause 5.8, and 10 CFR 50.34(f)(2)(v). Therefore, the staff finds the U.S. EPR interlock systems important to safety meet the requirements of IEEE Std 603-1998 Clauses 5.7, 5.8, and 6.5, and 10 CFR 50.34(f)(2)(v). Additional review of bypass and inoperable status indication is discussed in Section 7.5.4.2.1.1 of this report.

#### 7.6.4.4 *I&C and Control Room*

10 CFR Part 50, Appendix A, GDC 13, requires that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 19 requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss of coolant accidents. For the review of how the U.S. EPR design meets the requirements of GDC 13 and GDC 19, the staff used the guidance found in SRP Appendix 7.1 A and SRP Section 7.6.

FSAR Tier 2, Section 7.6.1.2, provides a functional description of the interlocks. The indications and alarms provided to the operator, as described in FSAR Tier 2, Section 7.6.1.2, verify correct operation of the interlock by providing information such as valve position, certain pressure and level measurements, alarms indicating conflicting occurrences, and pump status. FSAR Tier 2, Section 7.6.1.1, "System Description," states capability to perform manual actions related to interlocks is provided on the SICS. By having information provided to monitor interlocks over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions, the staff finds the U.S. EPR interlock systems important to safety adequately address the requirements of GDC 13. Section 7.6.4.3 of this report describes the surveillance and inoperable indication provided to the operator. The interlocks support actions to operate the nuclear power plant safely under normal conditions and maintain it in a safe condition under accident conditions. Therefore, the staff finds the U.S. EPR interlock systems important to safety adequately address the requirements of GDC 19. Further review of GDC 13 and GDC 19 is discussed in Section 7.5.4 of this report.

#### 7.6.4.5 *RCS Valve Interlocks*

10 CFR Part 50, Appendix A, GDC 15, requires, in part, that the RCS be designed with sufficient margin to assure that the design conditions of the RCS pressure boundary are not exceeded. SRP BTP 7-1 provides guidance on the isolation of low pressure systems from the

high pressure RCS. SRP BTP 7-1 states, in part, that the interfaces between low pressure and high pressure RCS should have the following features:

- At least two valves in series to isolate any subsystem whenever the primary system pressure is above the pressure rating of the subsystem.
- Systems where both valves are motor operated; the valves should have independent and diverse interlocks to prevent both from opening unless the primary system pressure is below the subsystem pressure. Also, valve operators should receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure.
- Suitable valve position indication should be provided in the control room.

To meet this guidance, FSAR Tier 2, Section 7.6.1.2.1, "RHR Suction Valve Interlocks," describes the RHR suction valve interlocks. Two motor operated isolation valves in series are interlocked to prevent opening when RCS pressure and temperature have not decreased below acceptable values. However, the applicant proposed an alternate method to SRP BTP 7-1, Position 2, which provides for an automatic signal to isolate the low pressure system from the high pressure RCS whenever primary system pressure exceeds the subsystem design pressure. In RAI 58 Question 07.06-1, the staff requested that the applicant clarify how the design addresses Position 2 of SRP BTP 7-1, Position 2. In a March 3, 2009, response to RAI 58 Question 07.06-1, the applicant stated that the following design features prevent an increasing pressure from exceeding the RHR system design pressure:

- Interlock holding the medium head safety injection (MHSI) large miniflow lines open
- Pressurizer safety relief valves operating in the low temperature over-pressure protection mode
- Spring loaded safety valves on the RHR suction lines

In follow-up RAI 286, Question 07.06-3, the staff requested that the applicant include certain aspects of the March 3, 2009, response to RAI 58 Question 07.06-1 in the FSAR. In a December 18, 2009, response to RAI 286, Question 07.06-03, the applicant stated that FSAR Tier 2, Section 7.6.1.2.4, would be revised to incorporate the following related information:

During a pressure increase due to the failed closed large miniflow valve of one of the MHSI pumps, by the time RCS pressure reaches the RHR safety valve opening setpoint, the three MHSI pumps with open large miniflow lines are no longer able to inject due to the higher RCS pressure caused by the single MHSI pump with its large miniflow valve closed.

This proposed revision to the FSAR is acceptable to the staff. RAI 286, Question 07.06-3, was being tracked as a confirmatory item. The staff has since verified that the change was made in FSAR Tier 2, Revision 2, Section 7.6.1.2.4 closing this confirmatory item.. Based on the above description, the staff finds that the U.S. EPR interlock systems important to safety adequately address 10 CFR Part 50, Appendix A, GDC 15.

SRP BTP 5-2, "Overpressurization Protection of Pressurized-Water Reactors While Operating at Low Temperatures," provides guidance on the overpressurization protection of pressurized



water reactors while operating at low temperature. SRP BTP 5-2 states, in part, that the system should be designed and installed to prevent exceeding the applicable technical specifications and 10 CFR Part 50, Appendix G, "Fracture Toughness Requirements," limits while operating at low temperatures. The system should be capable of relieving pressure during all anticipated overpressurization events at a rate sufficient to satisfy the technical specification limits, particularly while the RCS is in a water solid condition. LTOP should be operable during startup and shutdown conditions below the Appendix G limit temperature. To address this guidance, FSAR Tier 2, Section 7.6.1.2.4, "Interlocks to Provide Low Temperature Over-Pressure Protection," describes the interlocks providing LTOP. Low temperature RCS overpressure events include mass inputs and heat inputs. Additional details are provided in FSAR Tier 2, Section 5.2.2, "Overpressure Protection." The interlock is provided for two functions: (1) To support brittle fracture protection in case of a safety injection actuation during low temperature operation; and (2) To protect the RHR system from overpressure when connected to the RCS. FSAR Tier 2, Section 7.1.2.6.33, "Operating Bypass (Clauses 6.6 and 7.4)," states that the LTOP of the RCS is normally bypassed using P17 permissive when at power. During shutdown operations, LTOP protection is enabled when P17 is manually validated by the operator once the conditions for P17 are satisfied. Based on this design commitment, the staff finds that the U.S. EPR design addresses the guidance in BTP 5-2 by having interlocks to prevent over pressurization of the primary coolant system during low temperature operations. The U.S. EPR design addresses the guidance of BTP 5-2, as a means to meet the requirements of GDC 15.

SRP BTP 7-2, "Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines," provides guidance on requirements of motor operated valves (MOVs) in the ECCS accumulator lines. SRP BTP 7-2 states, in part, that the following features should be incorporated into the design of MOV systems for safety injection tanks:

- Automatic opening of the valves when either primary coolant system pressure exceeds a preselected value, or an SI signal is present
- Visual indication in the control room of the open or closed status of the valve
- Bypassed and inoperable status indication
- Utilization of the SI signal to remove automatically any bypass feature that may allow an isolation valve to be closed

To address this guidance, FSAR Tier 2, Section 7.6.1.2.2, "Safety Injection Accumulator Interlocks," describes the safety injection accumulator interlocks. Each accumulator is connected to the RCS through two check valves and a motor operated isolation valve in series. The PS provides automatic signals to open the accumulator isolation valves. Indications to the operator include pressure and level of each accumulator and the open or closed position of each accumulator isolation valve. An automatic "open" signal is sent to the accumulator isolation valves when SIS actuation occurs. FSAR Tier 2, Section 7.5.2.2.5, states that bypassed and inoperable status indication is provided for SI system accumulators. Based on these design commitments, the staff finds that the U.S. EPR design addresses the guidance of BTP 7-2. The U.S. EPR design addresses the guidance of BTP 7-2 as a means to meet the IEEE Std 603-1998 requirement that bypasses of a protective function will be removed automatically whenever permissives are not met.

SRP Section 7.6, major design consideration Item I, indicates that interlocks are required to isolate safety systems from non safety systems. FSAR Tier 2, Section 7.6, does not identify any safety to non-safety fluid system connections in the U.S. EPR design. The staff finds that the U.S. EPR design adequately addresses this design consideration.

SRP Section 7.6, major design consideration Item J, indicates that interlocks are required to preclude inadvertent inter ties between redundant or diverse safety systems. FSAR Tier 2, Section 7.6.1.2.3, "Interlocks Isolating Redundant CCWS Trains," describes two separate interlocks for the CCWS to prevent inadvertent inter ties between redundant safety systems. Interlocks are provided so that no two redundant CCWS trains are connected to the same common header at the same time and either the Common 1b or 2b headers can provide cooling to the RCP thermal barriers. Based on the design commitments in FSAR Tier 2, Section 7.6.1.2.3, the staff finds that the U.S. EPR design adequately addresses the design consideration.

### **7.6.5 Combined License Information Items**

No applicable items were identified in the FSAR. No additional COL information items need to be included in FSAR Tier 2, Table 1.8-2, for interlock systems important to safety consideration.

### **7.6.6 Conclusions**

The staff concludes that the design of the interlock systems is established in accordance with its safety function, is acceptable, and meets the relevant requirements of GDC 1, GDC 2, GDC 4, GDC 10, GDC 13, GDC 15, GDC 16, GDC 19, GDC 24, GDC 28, GDC 33, GDC 34, GDC 35, GDC 38, GDC 41, and GDC 44, 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h). The staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems.

The staff reviewed the single failure criterion and independence of safety interlocks. The staff finds that appropriate redundancy of interlocks satisfies single failure criterion. Independence from design basis events is provided by qualified equipment that operates in expected post event conditions. Certain sensor measurements passed to the non-safety-related system are through properly isolated connections. Therefore, the staff concludes the safety interlock system satisfies IEEE Std 603-1998, Clauses 5.6 and 6.3, and 10 CFR Part 50, Appendix A, GDC 24. Additional review of independence is discussed in Sections 7.1.4.10, 7.1.4.12.1, 7.1.4.12.3, and 7.9.4.5 of this report. Additional review of single failure protection is discussed in Section 7.1.4.5 of this report.

The staff reviewed the bypassed or inoperable status indication of safety interlocks. The staff finds that appropriate bypass indications are provided to give the operators timely information and status reports so the operators can mitigate the effects of unexpected system unavailability. Therefore, the staff concludes that the safety interlock systems satisfy the applicable requirements of IEEE Std 603-1998 and 10 CFR 50.34(f)(2)(v). Additional review of bypass and inoperable status indication is discussed in Section 7.5.4.2 of this report.

Based on the review of interlock system status information, initiation capabilities, and provisions to support safe shutdown, the staff concludes that information is provided to monitor interlocks over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for interlock initiation and bypass. The interlocks appropriately support actions to

operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the staff finds that the interlock systems satisfy the requirements of 10 CFR Part 50, Appendix A, GDC 13 and GDC 19. Additional review as related to control room is discussed in 7.5 of this report.

In the review of the interlock systems, the staff examined the dependence of this system on the availability of auxiliary supporting features and other auxiliary features. Based on this review and coordination with those having primary review responsibility of auxiliary supporting features and other auxiliary features, the staff concludes that the design of the interlock systems is compatible with the functional requirements of auxiliary supporting features and other auxiliary features.

SRP BTP 5-2 provides guidance on the over-pressurization protection of PWRs while operating at low temperature. SRP BTP 7-2 provides guidance on requirements of MOVs in the ECCS accumulator lines. The staff finds that interlocks are present to prevent over pressurization of the primary coolant system during LTOP and the interlocks for the SI accumulators have the required design features and, therefore, adequately address the guidance of SRP BTP 5 2 and BTP 7- 2. The U.S. EPR design addresses the guidance of BTP 7-2 as a means to meet the IEEE Std 603-1998 requirement that bypasses of a protective function will be removed automatically whenever permissives are not met. The staff finds that the U.S. EPR design adequately addresses the guidance of BTP 5 2 and, therefore, meets the requirements of GDC 15.

## **7.7 Control Systems Not Required For Safety**

### **7.7.1 Introduction**

The general objectives of the non-safety instrumentation and control systems are:

- To make sure the major process variables of the nuclear steam supply system are kept in predefined and allowed ranges during normal power operation
- To limit the variation of process parameters during normal operation in such a way that the initial conditions for operation are met at the onset of a DBE as assumed in the safety analyses
- To minimize the need for protective actions and thus increase plant availability
- To provide the reactor operator with monitoring instrumentation that indicates the required input and output control parameters of the systems and provide the operator with the capability of assuming manual control of the system

### **7.7.2 Summary of Application**

**FSAR Tier 1:** The FSAR Tier 1 information associated with Section 7.7 is found in FSAR Tier 1, Section 2.4.10, "Process Information and Control System," and Section 2.4.13, "Control Rod Drive Control System."

**FSAR Tier 2:** The applicant has provided a system description in FSAR Tier 2, Section 7. 7, summarized as the following.

In FSAR Tier 2, Section 7.7, "Control Systems Not Required for Safety," the applicant described I&C systems for normal plant operations that do not perform plant safety -related functions. However, these systems do control plant processes that have a significant impact on plant safety and control. This includes the main reactivity control of the nuclear reactor core with the positioning of the control rods, control of the feedwater, and regulation of reactor steam flow and pressure. These systems can affect the performance of safety-related functions either through normal operation, through inadvertent operation, or various anticipated operational occurrences.

While not directly essential to safe shutdown these systems must not prevent the safety function from operating when required. Further, the ability of these systems to meet the acceptance criteria also is dependent on quality software and human factors development which are outside the scope of this evaluation in this section. The control systems described in this Section include:

- Reactor control, surveillance, and limitation System
- Control Rod Drive System
- Process Automation System
- Neutron Monitoring System (NMS)

**ITAAC:** ITAAC: The ITAAC associated with FSAR, Tier 1, Section 7.7 are given in Table 2.4.10 1, "Process Information and Control System ITAAC," and Table 2.4.13 3, "Control Rod Drive Control System ITAAC."

**Technical Specifications:** There are no Technical Specifications for this area of review.

### **7.7.3 Regulatory Basis**

The relevant requirements of NRC regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, Section 7.7. "Control Systems," and are summarized below. Review interfaces with other SRP Sections also can be found in NUREG-0800, Section 7.6.

1. GDC 1, "Quality Standards and Records," as it relates to assuring structures, systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.
2. GDC 13, "Instrumentation and Control," as it relates to assuring Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems
3. GDC 15, "RCS (RCS) Design," to ensure the reactor coolant system and associated auxiliary, control, and protection systems design has sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition.

4. GDC 19, "Control Room," as it relates to providing a control room from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents.
5. GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.
6. GDC 28, "Reactivity Limits" as it relates to assuring that reactivity control systems are designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly the capability to cool the co.
7. GDC 29, "Protection Against Anticipated Operational Occurrences," as it relates to protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.
8. GDC 44, "Cooling Water," as it relates to assuring that a system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink is provided.
9. 10 CFR 50.55a(a)(1)
10. 10 CFR 52. 47(b)(1)

Acceptance criteria to meet the above requirements include:

SRP Table 7 1, Section 3 (Staff Requirements Memoranda), Section 4 (Regulatory Guides), and Section 5 (Branch Technical Positions), lists the SRP acceptance criteria applicable to control systems not required for safety.

#### **7.7.4 Technical Evaluation**

The objectives of the review are to confirm that control systems not required for safety conform to the staff's acceptance criteria and guidelines that the controlled variables can be maintained within prescribed operating ranges, and those effects of operation or failures of these systems are bounded by the accident analyses in Chapter 15 of this report.

Several of these design considerations are addressed in other sections of this report, as indicated in Table 7.7 1 below. The remaining major design considerations are discussed below. Additionally, the SRP lists other requirements applicable to interlock systems, including instrumentation and control available to operators, control room design, and bypass and inoperable status indication, which are addressed below.

**Table 7.7-1 Section 7.7 Design Considerations Referenced in Other Sections of this Report.**

<b>Design Consideration</b>	<b>Report Section(s)</b>
Quality of Components and Modules	7.1.4.7
Independence	7.1.4.10, 7.1.4.12.1, 7.1.4.12.3, 7.9.4, 7.9.4.5
Control Room	7.1.4.14, 7.1.4.23, 7.1.4.2.28, 7.4.4.1, 7.4.4.2
Clause 5.6	7.1.4.10
Clause 5.6.1	7.1.4.10.1, 7.9.4.5
Clause 5.6.2	7.1.4.12.2
Clause 5.6.3	7.1.4.12.3, 7.9.4.5
Clause 5.6.3.1	7.1.4.12.4
Clause 5.6.3.2	7.1.4.12.5
Clause 5.6.3.3	7.1.4.12.6
GDC 13 and GDC 19	7.1.4.3, 7.4.4.1, 7.4.4.2, 7.5.4.1.2, and 7.5.4.3
Qualification Programs	3.10, 3.11
GDC 1, GDC 2, GDC 4, GDC 15, GDC 16, GDC 28, GDC 33, GDC 34, GDC 35, GDC 38, GDC 41, GDC 44, 10 CFR 50.55a(a)(1)	7.1

10 CFR 50.55a(a)(3) allows an applicant under 10 CFR Part 52, to propose alternatives to the requirements of 10 CFR 50.55a(h) or portions thereof. The U.S. EPR design certification applicant proposes to use IEEE Std 603-1998, as an alternative to 10 CFR 50.55a(h) which requires the use IEEE Std 603-1991, Section 7.1.4.1 of this report discusses the staff evaluation and approval of this alternative.

At the time of the staff's review, the docketed version of the FSAR was Revision 2. However, in response to various RAIs, the applicant provided Interim Revision 3 mark-ups, that the staff used in preparing this report. Regarding the information in FSAR Tier 2, Section 7.7, the applicant provided Interim Revision 3 mark-ups for this section in a May 25, 2011, response to RAI 442, Question 07.01-28. In a June 22, 2011, response to RAI 452, Question 07.03-36, the applicant provided Interim Revision 3 mark-ups for FSAR Tier 1, Section 2.4. Upon receipt of the final Revision 3 of the FSAR, the staff will verify incorporation of the Interim Revision 3 mark-ups. **RAI 452, Question 07.03-36 is being tracked as a confirmatory item.**

#### **7.7.4.1      *System Description***

##### **7.7.4.1.1      *Rod Control and Rod Position Indication***

The components that are used to provide for rod control are the RCSL system, PICS, and CRDCS. PICS interfaces with the RCSL system to provide the operator with manual rod control capability. The RCSL system transmits the desired rod control movement direction and speed

to the rod control unit to the CRDCS. The CRDCS converts the demands from RCSL into rod movement current sequences supplied to the coils of the control rod drive mechanism.

Control rod bank insertion and withdrawal sequence and overlap are defined by the control bank insertion limits. Control rod banks are withdrawn and inserted in a prescribed sequence and overlap. For withdrawal, the sequence is Shutdown SA, Shutdown SB, Shutdown SC, Control A, Control B, Control C, and Control D. The insertion sequence is the reverse of the withdrawal sequence. The control bank rods move in a prescribed overlap that is specified in the core operating limits report. The rods move in the bank configuration for all cases except in the case of the partial trip. In a partial trip, the sub bank of rods that are dropped is a function of rod worth and relative position in the core.

During a reactor trip, the control rod drive mechanisms insert the drive rod and the attached RCCA by force of gravity. When a reactor trip signal occurs, the operating coils are de-energized. The CRDCS is primarily classified as non-safety-related. The exception is the trip contactors within the CRDCS, which are safety-related. The CRDCS has the following safety-related functions:

- interrupts power to the CRDMs via the reactor trip contactors
- provides signals that report the status of the reactor trip contactor modules to the PS

The CRDCS also provides a non-safety-related function to actuate the RCCAs through the CRDMs.

The CRDMs are equipped with a digital and analog position indication system so the RCCA position is measured over the height of the core by two diverse methods:

- A digital measurement which is non safety related
- An analog measurement that is safety related

Additionally, an upper and lower rod position indicator provides indication when the RCCA is at the top or bottom position. A feedback signal from the CRDCS rod control unit to the RCSL system provides information necessary for digital position indication of the RCCA based on the number of rod movement steps sent to the RCCA.

The RCSL system is implemented with the TXS digital I&C platform. The RCSL system transmits commands containing the direction of movement (i.e., withdrawal or insertion), speed of movement, and drop and hold information to the CRDCS. The RCSL systems are organized into four divisions located in separate Safeguard Buildings. The RCSL system is powered from the 12 UPS. The RCSL is classified as a non-safety-related-system and performs two types of core control functions: Operational Control and Limitation Control. Operational control functions provide control of plant systems during normal operation. These functions are used to make sure the major process variables are kept in predefined and allowed ranges during normal power operation. Limitation control functions either prevent plant disturbances from causing normal operating limits to be exceeded, alert the operator when normal operating limits have been exceeded, or prevent disturbances from leading to a DBE. The following is a summary of the operational and limitation controls.

## Operational Control Functions

- Average Coolant Temperature Control maintains a programmed RCS average temperature ( $T_{avg}$ ) by regulating core power. The Average Coolant Temperature Control is the predominant function of core control.
- Neutron Flux Control regulates reactor power (i.e., neutron flux) during startup and shutdown operations, while the secondary pressure is controlled with the turbine bypass system. This function simplifies the constant power operation and facilitates the operator tasks during the startup of the turbine and the synchronization of the generator with the grid.
- Axial Offset Control maintains core axial power within analyzed limits. Axial offset is a measure of the axial power distribution in the core.

## Limitation Control Functions

- Loss of One Reactor Coolant Pump Limitation initiates a partial trip and a turbine load reduction when two RCS loop flow values of the same loop drop below the setpoint value, and the P3 permissive is validated. This limitation function is designed to avoid the low reactor coolant flowrate reactor trip.
- Axial Offset Limitation surveys the axial power imbalance to ensure the axial power distribution is within the parameters assumed in the safety analysis to limit the consequences at high power levels of accidents for which a top peaked core power distribution is penalizing. This function generates alarms and the blocking of power increase.
- Reactor Power Limitation with Respect to Feedwater Flow Rate limits the reactor power with respect to the feedwater flowrate. The limitation function is designed to correct plant conditions before a protective action due to low SG level occurs.
- Reactor Power Limitation with Respect to Generator Power limits reactor power after loss of generator load events by initiating a partial-trip.
- Reactor Power Limitation with Respect to Thermal Power maintains reactor power below 100 percent rated thermal power. This function provides the capability to adjust turbine power and indirectly reactor power due to cooling tower temperature changes that affect overall plant efficiencies.
- Rod Drop Limitation detects the spurious drop of RCCA(s) and to reduce the turbine generator power level to match the reactor power reduction due to the dropped RCCAs.
- Intermediate Range High Neutron Flux Limitation reduces the necessity of a high neutron flux (i.e., intermediate range) and low doubling time (i.e., intermediate range) reactor trips when an excessive reactivity increase occurs during reactor startup from a subcritical or a low power startup condition. At the limitation criteria, the withdrawal of any RCCA is blocked.
- High Linear Power Density Limitation reduces the necessity of a reactor trip on HLPD for each transient that leads to an uncontrolled increase of the linear power density of the reactor core. This function initiates a partial trip and a fast turbine load reduction.



- Low Departure from Nucleate Boiling Limitation corrects conditions that may lead to low DNBR protective actions. The functions provide DNBR margin with respect to the DNB criterion.
- RCS Boron Dilution (Shutdown Condition) Limitation is designed to avoid the actuation of the anti dilution in standard shutdown protective action.

#### 7.7.4.1.2 *Process Automation System*

- The PAS is the main automation and control system for the plant. The PAS provides controls for both safety-related and non-safety-related equipment. As a non-safety-related system, PAS only implements non-safety-related or non-credited control functions for safety-related systems.
- The PAS performs operational and limitation I&C functions except those performed by RCSL or the TG I&C system. The PAS also executes those risk reduction I&C functions required to mitigate beyond design basis events other than severe accidents, including station blackout mitigation. PICS interfaces with PAS to provide operator control and monitoring capability of plant parameters.
- The PAS executes manual component level control of safety-related process systems initiated from the PICS. PAS performs the following automatic plant control and limitation functions:
- RCS Pressure Control and Limitations maintains the RCS pressure within allowable limits during Mode 1 through Mode 5. When in the automatic control mode, the RCS pressure control maintains the primary pressure at a setpoint value in steady state operation and within an allowable range around its setpoint (i.e., control band) during transients, including startup and cooldown operations.
- Pressurizer Level Control maintains the pressurizer level at a setpoint value in steady state operation and within the allowable range around its setpoints during normal operational situations, including startup and cooldown. When in automatic control mode, pressurizer level control channel ensures that the pressurizer level remains within specified limits (i.e., control band) around the setpoint. A manual control mode allows manual setpoint control and manual control of the pressure reducing valve actuators.
- RCS Loop Level Control and Limitation Function provides an automatic and continuous control of the RCS water inventory during mid loop operation. In case of primary system inventory changes, the control function limits the resulting mid loop operation level deviations within the specified control band.
- SG Water Level and Feedwater Control and Limitation Functions automatically maintain SG level by matching feedwater flow to steam demand. The level can also be controlled manually. The SG level control I&C function maintains the SG level at a setpoint value in steady-state operation during heatup and cooldown (Mode 1 through Mode 4), and within allowable limits (called the control band) during normal operational transients.
- Main Steam Pressure Control provides main steam overpressure control and limitation in case of load reduction due to load steps, load ramps, or load rejection. Main steam pressure is controlled by automatically modulating the turbine bypass valves.

- Residual Heat Removal System Function protects the RHR system equipment from over pressurization and prevents challenging the pressurizer safety relief valves during low temperature operation. The setpoint for the RHR system function is below the RHR system maximum pressure.
- Reactor Coolant Pump Function reduces the necessity of a reactor trip on low pressurizer pressure during Mode 1. It also protects RCPs from cavitation and keeps pressure from falling below the setpoint for initiation of safety injection. The RCP function setpoint is temperature dependent and below the nominal operating pressure setpoint of the RCS pressure control function. The function is operational in Mode 1 through Mode 5.
- Reactor Pressure Vessel Brittle Fracture Function protects the RCS from over pressurization. The lowering of the pressurizer safety relief valve opening setpoints is performed by the PS. The RPV brittle fracture function is implemented in the PAS to prevent pressure from reaching the electrically controlled relief valve opening setpoints when in Mode 4 and Mode 5. The reactor pressure vessel brittle fracture setpoint is temperature dependent.
- Pressurizer Level Limitation Functions are designed to back up the normal pressurizer level control function when the normal control function is outside of its normal control band. This process is achieved by performing actions that supplement the normal control function to return the RCS to the 100 percent power, level control band following a transient causing the deviation. This improves the availability of the plant by correcting pressurizer level before reaching reactor trip setpoints and other safety protective function setpoints.

#### *7.7.4.1.3 Neutron Monitoring Systems*

The neutron monitoring systems consists of the ICIS and the EIS. The ICIS consists of safety-related and non-safety-related equipment. The ICIS consists of:

- Self powered neutron detectors (safety-related except for test equipment)
- Aeroball measurement system (non-safety-related)
- Fixed core outlet thermocouple measurement system (safety-related)
- Reactor pressure vessel dome temperature measurement system (non-safety-related)

There are 72 SPNDs that continuously measure the neutron flux at specified positions in the core to provide information about the three dimensional flux distribution. The AMS is used to calibrate the SPNDs at regular intervals.

The COTs continuously measure fuel assembly outlet temperature. The fixed thermocouples are placed in selected fuel assemblies that are located azimuthally and radially within the core. The core outlet temperature is used to determine the saturation margin at the core exit and provide information about the radial temperature distribution in the core and average temperature in the RCS. There are a total of 36 COTs. The COTs are arranged with three thermocouples (two narrow range thermocouples and one wide range thermocouple) within each of the twelve SPND finger assemblies.

The RPVDT measurement system continuously measures the temperature within the reactor dome. The sensing elements are thermocouples, which are passive devices that do not use electrical power. RPVDT instrumentation provides temperature signals corresponding to the top level, mid level, and bottom level measurement regions of the dome. The measurements of fluid temperature in the RPV dome provide information to the operator during normal and emergency operations if they are available (although not required for post-accident monitoring). The main functions of the dome thermocouples are to:

- indicate a potential steam bubble
- indicate average dome temperature
- indicate temperature above RCCA plate to determine temperature difference across the plate
- indicate air temperature during RCS venting during startup

The EIS monitors neutron flux during power and shutdown modes of operation. Since it is not possible to measure the entire operating range of reactor power with a single instrument, the following three ranges of detection are used.

- Power range – uses an uncompensated, boron lined ionization chamber detector
- Intermediate range – uses a gamma compensated, boron lined ionization chamber detector
- Source range – uses a boron lined proportional counter detector

There are eight power range detectors that cover the upper three decades up to 200 percent reactor power. Two detectors are located in each of four radial locations around the core (45°, 135°, 225°, 315°). The two detectors at each location measure the center of the upper and lower portions of the core for monitoring and control of axial flux distributions. Four intermediate range detectors monitor a little more than seven decades up to at least 60 percent full power, with an overlapping of the source range by about 2.5 decades. They are located in the same radial locations as the power range detectors. Three source range detectors are provided at three radial locations around the core (0°, 90°, 270°). The source range monitors the lower six decades. Overlaps in the measuring ranges are provided to allow operation of each range during transitions in power levels. These ranges provide coverage from shutdown conditions to about 200 percent reactor power.

#### *7.7.4.1.4 Leak Detection System*

The leak detection system, in conjunction with other associated systems, promptly detects, quantifies, and localizes leakage from the RCS pressure boundary and selected portions of the main steam system.

The leak detection system includes: (1) Condensate mass flow measurement devices inside containment; (2) Humidity and temperature sensors inside containment; and (3) Local humidity detection system for main steam piping. The local humidity detection system measures local increases in relative humidity along appropriate portions of the main steam lines inside of the containment to detect and localize leakages from the lines with a high degree of accuracy. The leak detection system is classified as non-safety-related.

#### *7.7.4.1.5 Vibration Monitoring System*

The vibration monitoring system monitors changes in the vibration behavior of the reactor pressure vessel and its internals, the primary system components, the main coolant pumps, and portions of the main steam line structures in the secondary system by monitoring the frequencies and amplitudes of service induced component and fluid vibrations. Change in the vibration behavior of a structure or component is one of the most sensitive indicators of a condition change such as reduction of screw bolt pretensions, reduction in the stiffness of core barrel hold down springs, direct contact between primary components and the containment building, damage to main coolant pump bearings, and cracks in the main coolant pump shaft. The vibration monitoring system is classified as non safety related.

#### *7.7.4.1.6 Loose Parts Monitoring System*

The loose parts monitoring system detects, locates, and analyzes detached or loosened parts and foreign bodies in the RCS and the secondary side of the SGs during normal plant operation. By providing an early detection of loose parts, the probability of primary or secondary system component damage can be lessened and exposure to station personnel can be minimized. The loose parts monitoring system is classified as non-safety-related.

#### *7.7.4.2 Control System Quality Assurance*

The requirements of 10 CFR 50.55a(a)(1) address quality standards for systems important to safety and requires that SSCs must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. 10 CFR Part 50, Appendix A, GDC 1, "Quality Standards and Records," requires, in part, that a quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. The staff used the guidance of SRP Section 7.7 to evaluate each control system for conformance to the stated quality criterion. The guidance of SRP 7.7 states that control system software should be developed using a structured process similar to that applied to safety system software. Elements of the review process may be tailored to account for the lower safety significance of control system software. In addition, SRP 7.7 states that I&C control systems include environmental control as necessary to protect equipment from environmental extremes. The following Sections document the staff's quality assurance evaluation for applicable U.S. EPR I&C non-safety related control systems.

##### *7.7.4.2.1 Reactor Control, Surveillance, and Limitation System Quality Assurance*

The FSAR Tier 2, Section 7.1.1.4.5, Interim Revision 3 mark-ups, states that the RCSL is implemented with the TXS digital platform. The staff's safety evaluation report of Topical Report EMF-2110, "TELEPERM TM XS: A Digital Reactor Protection System," Revision 1, states the following in Section 5.0:

10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety," is addressed by conformance with the codes and standards listed in the SRP. Siemens [vendor of TXS at the time of the staff's review] uses codes and standards in the development of the TXS system that are the same as or equivalent to the standards in the SRP and, therefore, the TXS system is in conformance with this requirement.

and

Based upon the review of the safety system designs for conformance to the guidelines, the staff finds that there is reasonable assurance that the TXS system conforms to the guidelines applicable to these systems. Therefore, the staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

FSAR Tier 2, Section 7.1.1.4.5, Interim Revision 3 mark-ups, states that equipment used in the RCSL will be rated by the manufacturer to operate under the mild environmental conditions expected to exist at its location during the events that the equipment is expected to be used. RCSL equipment quality is required to be consistent with the quality assurance plan for non-safety-related equipment as described in Topical Report ANP-10266, Addendum A. In the Safety Evaluation Report for Topical Report ANP-10266 (ML071790218), Section 4.0, the staff concluded that the applicant's QAP complies with the applicable NRC regulations and industry standards and can be used by the applicant for design certification activities associated with the EPR. Accordingly, based on the staff's safety review for quality assurance and acceptance of the TXS digital platform and Topical Report ANP-10266, Addendum A non-safety-related QAP, the staff finds that GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed for the TXS-based RCSL system.

#### *7.7.4.2.2 Control Rod Drive Control System Quality Assurance*

FSAR Tier 2, Revision 2, Section 7.1.2.2.1, states that I&C systems listed in FSAR Tier 2, Table 7.1-2 shall be designed to meet the requirements of GDC 1. FSAR Tier 2, Table 7.1-2, "System Requirements Matrix," identifies that the CRDCS will be designed to the requirements of regulatory criterion 10 CFR 50.55a(a)(1) and GDC 1. FSAR Tier 2, Section 7.1.1.5.1, states that the non-safety-related components of the CRDCS are designed such that a seismic event does not result in damage that disables the safety function of the trip contactors and that the non-safety-related CRDCS equipment will be designed, procured, installed, and tested in accordance with the QAP for non-safety-related equipment as described in Topical Report ANP-10266, Addendum A. Accordingly, the staff finds that the applicant's non-safety-related quality design descriptions and quality assurance commitments for the non-safety-related CRDCS equipment meet the applicable quality requirements of GDC 1 and 10 CFR 50.55a(a)(1). The safety-related portion of CRDCS is discussed in Section 7.1.4 of this report.

#### *7.7.4.2.3 Process Automation System Quality Assurance*

FSAR Tier 2, Section 7.1.1.4.6, Interim Revision 3 mark-ups, states that the PAS equipment quality requirements will be consistent with the QAP for non-safety-related equipment as described in Topical Report ANP-10266A, Addendum A. The staff's approval of this non-safety-related QAP is discussed in Section 7.7.4.2.1 of this report. The PAS will be implemented with a commercial grade I&C platform. Accordingly, the staff concludes that the PAS QA requirements comply with the applicable requirements of GDC 1 and 10 CFR 50.55a(a)(1).

#### *7.7.4.2.4 Process Information and Control System Quality Assurance*

FSAR Tier 2, Section 7.1.1.3.2, "Process Information and Control System," Interim Revision 3 mark-ups, states that the design of the PICS is accomplished through a phased approach consisting of the following phases:

- System requirements phase
- System design phase

- Software/hardware requirements phase
- Software/hardware design phase
- Software/hardware implementation phase
- Software/hardware validation phase
- System integration phase
- System validation phase
- Verification and validation of the PICS software is performed
- PICS requirements are documented in a traceable form via configuration management
- PICS design is validated through acceptance test in the system validation phase

In addition, the design, fabrication and testing of PICS equipment will follow the approved non-safety-related QAP in Topical Report ANP-10266, Addendum A.

FSAR Tier 2, Section 7.1.1.3.2, states that PICS equipment is located in safeguard buildings that provide a mild environment during and following DBEs and will be rated by the manufacturer to operate under the mild environmental conditions expected to exist at its location during the events that the equipment is expected to be used. However, the staff noted that the statement in parenthesis, “(or otherwise reasonably expected),” does not present a clear commitment for environmental qualification of PICS and should be removed unless otherwise clarified. Therefore, in RAI 505, Question 07.07.23, the staff requested that the applicant to remove, or further clarify, this statement. **RAI 505, Question 07.07-23 is being tracked as an open item.**

Except for RAI 505, Question 07.07-23,, the staff finds the quality assurance for PICS design, fabrication, development plans, and testing commitments, meet the requirements of GDC 1 and 10 CFR 50.55a(a)(1).

#### 7.7.4.3 *Control System Design Basis Evaluation*

The following sections document the staff's evaluation of each applicable non-safety-related control system for conformance to the applicable general design criteria. The staff used the guidance of SRP Section 7.7 to evaluate each control system for conformance to the listed criterion.

##### 7.7.4.3.1 *RCSL Design Bases Evaluation*

###### 7.7.4.3.1.1 Maintaining Plant Variables within Predefined and Allowable Ranges

10 CFR Part 50, Appendix A, GDC 10, "Reactor Design," requires, in part, that the reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. GDC 15, "RCS Design," requires that the RCS and associated auxiliary, control, and protection system will be designed with sufficient margin to ensure that the design conditions of the reactor coolant

pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.

FSAR Tier 2, Revision 2, Section 7.7, states that the objectives of the non-safety-related I&C control systems are to make sure the major process variables are kept in pre-defined and allowed ranges during normal power operation to prevent plant disturbances from causing normal operating limits to be exceeded and to prevent disturbances from leading to a design basis event. The RCSL system is credited with providing the actuation signals for control rod movement direction (i.e., insertion or withdrawal) and control rod movement speed. By initiating or blocking control rod movement, the RCSL helps to control the addition or removal of reactivity to reactor power, and thus, the increase or decrease of reactor power. The RCSL system has the ability to limit reactor power by initiating a partial trip of the control rods. The RCSL system also controls reactor power by controlling the concentration levels of boron (a neutron absorber) within the RCS. Boron addition and dilution signals are generated by RCSL and are sent to the chemical and volume control system for boron addition or dilution actuation.

FSAR Tier 2, Revision 2, Section 4.3.2.4.5, states that there is a control rod insertion allowance that, at full power, the control bank of rods are operated within a prescribed band of travel to compensate for small changes in boron concentration, changes in moderator temperature, and the changes in xenon concentration that are not compensated for by the changes in boron concentration. When the control bank reaches the limit of this band, a change in boron concentration is required to compensate for any additional reactivity changes. FSAR Tier 2, Section 4.3.1.7, states that the maximum rate of reactivity insertion utilizing control rod movement is limited. The control rod maximum speed withdrawal rate is 75 steps/minute. Since each rod movement step equals 0.99822 cm/step (0.393 in./step), the maximum withdrawal rate of the control rod is 74.8792 cm/minute, (29.48 in./minute) which is less than the maximum allowed of (76.2 cm/minute (30 in./minute) in the Chapter 15 safety analysis. Table 7.7-1 below list the parameters that the RCSL system monitors to control reactor power.

**Table 7.7-2 RCSL Control Features<sup>1</sup>**

<b>Variable Monitored</b>	<b>RCSL Generates Signals to</b>	<b>Design Basis</b>
Neutron Flux Control	Initiate control rod movement	Control reactor power during startup and shutdown operations
Average Coolant Temperature	Initiate control rod movement, boron addition or dilution and/or block turbine power increase or decrease	Maintain programmed RCS average temperature (Tavg)
Core Power Axial Offset Control	Block rod movement; Initiate or block boron dilution	Maintain core axial power within analyzed limits
Loss of One Reactor Coolant Pump	Initiates a Partial Trip (PT) and a turbine load reduction	Avoid the low reactor coolant flowrate reactor trip
Axial Offset Limitation	Blocking generator power increase	Keeps axial power distribution within parameters

---

<sup>1</sup> Table created from RCSL design descriptions contained in FSAR Tier 2, Section 7.7, "Control Systems Not Required for Safety," Interim Revision 3 Mark-ups.

<b>Variable Monitored</b>	<b>RCSL Generates Signals to</b>	<b>Design Basis</b>
Loss of One MFW Pump	Initiate a PT and turbine load reduction	Correct plant conditions before a protective action due to low S/G level
Loss of All MFW Pumps	Initiate reactor trip, turbine trip, close all FW Full load control valve (FLCV)	Correct plant conditions before a protective action due to low S/G level
Imbalance of Feedwater Flowrate and Rx Power During Startup	Blocking withdrawal of any control rods	Prevent increase in Rx power without an increase of MFW flowrate
Reactor Power Limitation for loss of Generator Load Events	Initiate a PT	Limit the energy level of the primary system in case of load rejections or turbine trip in order to avoid reaching the RT setpoint
Reactor Power Limitation for Thermal Power	Adjust turbine power	Maintain reactor power below 100% rated thermal power
Rod Drop Limitation	Reduce turbine generator power level	Reduce the generator power to match the Rx power reduction due to dropped rod(s)
Intermediate Range High Neutron Flux Limitation	Block rod withdrawal	Avoid high neutron flux and low doubling time reactor trips during Rx start-up
High Linear Power Density Limitation	Initiates PT and fast turbine load reduction	Avoid a reactor trip on High Linear Power Density
Low Departure from Nucleate Boiling Limitation	Block rod withdrawal, reduce power, and/or initiate PT	Correct conditions to avoid the low departure from nucleate boiling ratio protective actions

The neutron flux control function is designed to control reactor power during startup and shutdown operations, while secondary pressure is being controlled with the turbine bypass system. The neutron flux control function is used below 25 percent reactor power. Reactor core neutron flux is compared to a neutron flux control function setpoint. The neutron flux control function blocks turbine synchronization at power levels less than the neutron flux control setpoint when increasing reactor power from startup and blocks power reductions below the neutron flux control setpoint until the turbine is tripped on decreasing reactor power.

At reactor power levels greater than 25 percent, the average coolant temperature (ACT) control function is used instead of the neutron flux control function. The ACT control function is designed to maintain a programmed RCS average coolant temperature (Tavg) by regulating core power. The ACT control function consists of two main error signal channels that are summed to provide a total error input signal to the rod speed control program. The signal output of the rod speed program is a digital pulse that determines both rod stepping speed and direction (i.e., insertion or withdrawal). The two error channels are:



- Average temperature error - Difference between the second highest (auctioneered) measured loop Tavg and the ACT setpoint.
- Power imbalance feed-forward error - Mismatch between turbine generator load and reactor power.

Incoming sensor and detector signals are acquired in the acquisition units (AUs) from the SCDS. There are four redundant AUs in RCSL, one in each division. There are two redundant control units in RCSL, one in Division 1 and one in Division 4. Each CU is connected to all four AUs. The two CUs operate in a master/hot-standby configuration, where the signals are processed and signal selection is performed in the CUs.

The signal selection algorithm program within the CUs is programmed to select a parameter value from plant sensors on which to base process control actions. The controlling process values are selected from multiple input signals. The selected value is based on intermediate values of the process variable so that extreme values (min or max) are ignored. This control method is credited to reduce the possibility of the control system acting on an erroneous extreme value, as may result from instrument or other failures. The power imbalance feed-forward error signal and the temperature error signal are summed together to produce a total error signal. This total error signal is the output that determines whether the control rods need to be inserted or withdrawn and the speed at which the rod movement occurs. If the total error is negative, rods are withdrawn. If the total error is positive, rods are inserted. If a control rod axial offset limit is encountered (i.e., control rod movement will be blocked or prevented) the ACT system will automatically switch to boron addition and dilution batches as the method to perform the ACT function. When rod movement is prohibited and the total error is positive, a boron addition batch will be performed, and when rod movement is prohibited and the total error is negative, a dilution batch will be performed. The RCSL axial offset rod control function is designed to maintain core axial power within analyzed limits. Axial offset is a measure of the axial power distribution in the core. During increasing reactor power operations, automatic rod withdrawal is blocked when the core power axial offset exceeds the positive axial offset band limit (i.e., boron dilution batch will perform ACT control). When a negative axial offset limit is exceeded, automatic boron dilution is blocked and the RCSL will use automatic rod withdrawal to perform ACT control.

There are two phases of axial offset control bands. The previous paragraph describes the first phase axial offset control band. In the first phase the axial offset control band implements restrictions on rod motion to attempt to control core power axial offset within the first phase band. During the second phase axial offset control band, when increasing reactor power, if the core axial offset power exceeds the second phase axial offset band limits, all automatic dilutions, rod withdrawal, and power increases are blocked. During decreasing reactor power operations, the process is reversed.

The guidance of SRP Appendix 7.1-A Item 2, Paragraph (d) and (f), states, in part, that the I&C systems may contribute to RCS design margin by providing better than the minimum required performance, as conservatism in setpoint calculations, or by system features that make the protection or control systems more fault tolerant. The staff concludes that the design feature of redundant CUs provided in both Divisions 1 and 4, which prevent the failure of a single CU from disabling control rods, adds to the overall fault tolerance of the RCSL system. As discussed above, by keeping reactor core parameters within defined operating ranges, this will prevent plant fluctuations from exceeding safety system setpoints and safety system automatic actuations. FSAR Tier 2, Table 7.1-2, "System Requirements Matrix," Interim Revision 3

mark-ups, identifies that the RCSL will be designed to the requirements of GDC 10 and GDC 15. Therefore, the staff finds that these design features would make the RCSL control features fault tolerant to postulated system failures would contribute to the RCS design margin, and thus, meet the requirements of GDC 10 and GDC 15.

#### 7.7.4.3.1.2 RCSL Instrumentation to Monitor and Control Plant Variables and Systems

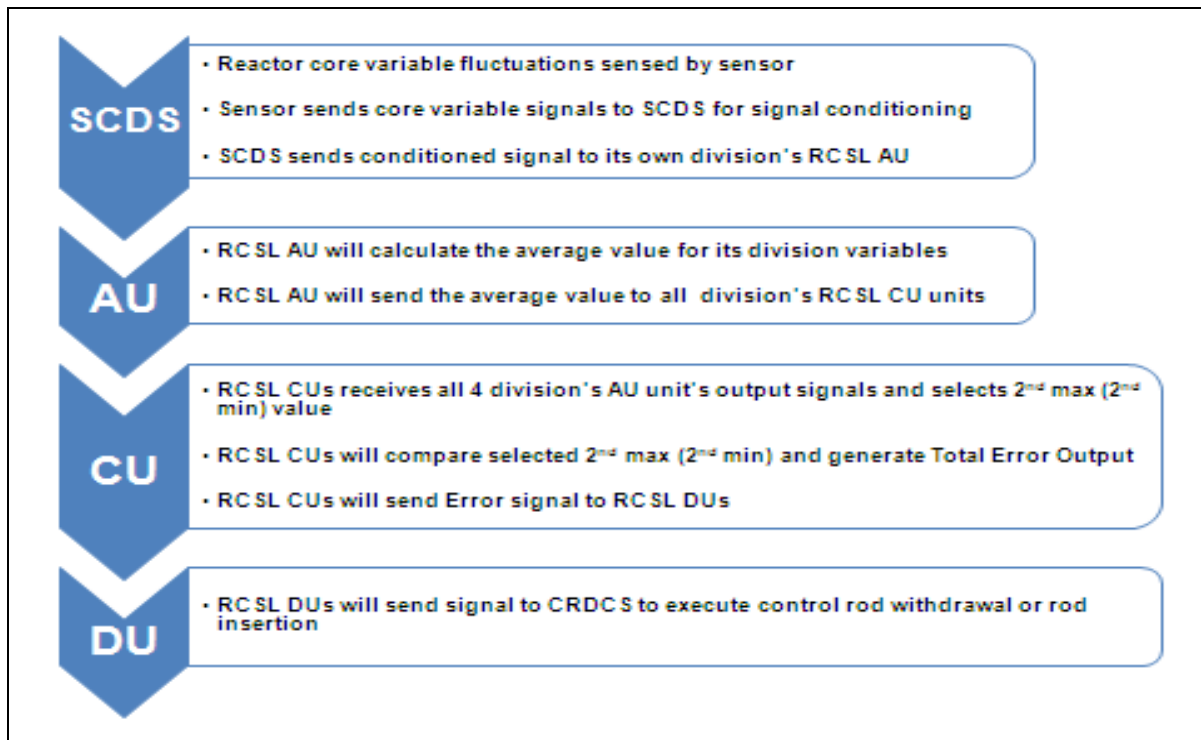
GDC 13, "Instrumentation and Control," requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. GDC 19, "Control Room," requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions.

The staff applied the guidance of SRP Appendix 7.1-A to review the RCSL instrumentation for conformance to GDC 13. The guidance of SRP Appendix 7.1-A states that the review for compliance with GDC 13 should include consideration of

- the instrumentation to monitor plant variables and systems
- the I&C to maintain variables and systems within normal operational limits
- setpoints for instrumentation system alarms and control system actions

FSAR Tier 2, Section 7.7.1.1, Interim Revision 3 mark-ups, states that the RCSL system receives input signals from the SCDS and implements the automation level I&C functions related to core control. An example of an I&C signal path for an RCSL monitored reactor core parameter from sensor to the CRDCS input is shown in FSAR Tier 2, Figure 7.7-6, Interim Revision 3 mark-ups.

The signal selection algorithms contained in the CUs filters the values such that control of the process is based on intermediate values of the process variable so that extreme values (i.e., extreme minimums or maximums) are ignored. FSAR Tier 2, Section 7.7.2.6, Interim Revision 3 mark-ups, states that the control systems functions maintain the process variables in predefined ranges during normal operation. FSAR Tier 2, Section 7.7.3, Interim Revision 3 mark-ups, states that control system conditions are designed to prevent undesirable conditions in the operation of the plant such that if this condition were reached, it would require safety-related actions by the PS. The range of control operation for the RCSL is designed to adjust, stop, or initiate control rod positioning within the core, initiate a partial trip, perform turbine load reduction and/or initiate boron dilution or addition, to prevent a safety-related PS setpoint from being reached. In addition, FSAR Tier 2, Table 7.1-2, Interim Revision 3 mark-ups, identified GDC 13 is a requirement for the design of the RCSL. Based on the listed figures and the



**Figure 7.7-1 I&C Signal Flow Path From Sensor to Control Rods<sup>2</sup>**

design descriptions explaining the instrumentation process flow and the instrumentation provided to maintain plant parameters and processes within defined ranges, the staff concludes that the applicant's design for the RCSL addresses the guidance of SRP Section 7.7 and SRP Appendix 7.1-A for sufficiency of instrumentation to monitor and control plant variables and systems. Accordingly, the staff finds that the RCSL meets the requirements of GDC 13.

The guidance of SRP Appendix 7.1-A, states that for applicability of GDC 19, the review should address the I&C available to operate the nuclear power plant under normal and accident conditions. FSAR Tier 2, Section 7.7.1.1, states that PICS interfaces with the RCSL system to provide the operator with control and monitoring capability of the core control functions. PICS equipment is located in the MCR and the RSS. The operators can manually adjust monitored plant parameter's control setpoints from the PICS in the MCR. Control rod position within the core, as well as scram and PT positions, are sensed by the RCSL and displayed on the PICS. Alarms that are generated by the RCSL are sent to the PICS to alert the operators. The accident analysis does not credit non-safety related systems to provide protection. However, if available, the operators are able to continue using these systems if needed. The plant alarm annunciator is integrated into the PICS operating and monitoring system. Special screens display and organize alarms and warnings based on their status and relative level of importance. An alarm hierarchy with a color coding system is used to alert the operator of the importance of the alarm based on the relevance to plant safety.

<sup>2</sup> RCSL I&C path flowchart created from FSAR Tier 2. Figures 7.1-10 and 7.7-6, Interim Revision 3 Mark-ups.

Based on the listed RCSL display and alarms provided to the operator in the MCR on the PICS, the staff concludes that the RCSL design provides sufficient instrumentation to the operator in the MCR and addresses the guidance of SRP Appendix 7.1-A for GDC 19 I&C available to the operator for both normal and accident conditions. Accordingly, the staff finds that the RCSL meets the requirements of GDC 19.

#### *7.7.4.3.2 CRDCS Design Bases Evaluation*

##### *7.7.4.3.2.1 Maintaining Plant Variables within Predefined and Allowable Ranges*

10 CFR Part 50, Appendix A, GDC 10, "Reactor Design," requires that the reactor core and associated coolant, control, and protection systems be designed with appropriate margin to assure that specified fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. 10 CFR Part 50, Appendix A, GDC 15, "RCS Design," requires the RCS and associated auxiliary, control, and protection system be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.

The CRDCS provides the interface with the RCSL system for control of reactor control rod movement. FSAR Tier 2, Section 7.7.1.1, Interim Revision 3 mark-ups, states that the RCSL logic sends the control rod movement direction, speed of movement, and drop and hold signals to the rod control units of the CRDCS. Each CRDCS rod control unit generates the cycling sequence and rod speed for its control rod, which is used as the input to the CRDM coil modules. A feedback signal from the rod control unit to the RCSL system provides information necessary for digital position indication of the control rod based on the number of rod movement steps sent to the control rod. The CRDCS controls and measures the current to each CRDM coil. There is a coil module in the CRDCS for each CRDM coil. This module controls the amount of current applied, as well as provides the correct sequencing of coil currents for control rod movement insertion or withdrawal out of the core. FSAR Tier 1, Section 2.4.13, Interim Revision 3 mark-ups, states that the CRDCS reactor trip contactors listed in FSAR Tier 1, Table 2.4.13-1 can perform their safety function when subjected to EMI, RFI, electrostatic discharges, and power surges. FSAR Tier 1, Interim Revision 3 mark-ups, Table 2.4.13-3, Item 4.4, ITAAC acceptance criteria, states that the CRDCS limits the control rod bank withdrawal rate to 76.2 cm/minute (30 in./minute) or less. The control rod maximum speed withdrawal rate is 75 steps/minute. Since each rod movement step equals 0.9982 cm/step ((0.393 in./step), the maximum withdrawal rate of the RCCA is 74.8792 cm/minute (29.48 in./minute) which is less than the maximum allowed of 76.2 cm/minute (30 in./minute). The safety-related reactor trip contactors in the reactor trip contactor module open when reactor trip signals from at least two of the four PS divisions are received by the reactor trip contactor module.

FSAR Tier 2, Table 7.1-2, Interim Revision 3 mark-ups, identifies that the CRDCS will be designed to the applicable regulatory criteria of GDC 10. As described, above, the CRDCS works in conjunction with the RCSL to provide reactivity control and limitations to prevent unnecessary challenges to the safety functions. Accordingly, the staff finds that the CRDCS meets the applicable requirements of GDC 10 and GDC 15.

#### 7.7.4.3.2.2 CRDCS Instrumentation to Monitor and Control Plant Variables and Systems

GDC 13, "Instrumentation and Control," requires that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. GDC 19, "Control Room," requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions.

The staff applied the guidance of SRP Appendix 7.1-A to review for conformance to GDC 13. The guidance of SRP Appendix 7.1-A states that the review for compliance with GDC 13 should include consideration of

- the instrumentation to monitor plant variables and systems
- the I&C to maintain variables and systems within normal operational limit
- setpoints for instrumentation system alarms and control system actions

In order to control the amount of reactivity inserted into the core by the control rods and maintain reactor core parameters within analyzed limits, the rate of control rod movement must be regulated and limited. FSAR Tier 2, Revision 2, Section 3.9.4.1.1.4, states that the position of each control rod is measured by an analog and a digital position indicator system that is located on the outside of the CRDM pressure housing. The coil housing assembly, which contains the gripping coil, the lifting coil, and the holding coil, is combined with the position indicator coils and a sheet steel casing to form a single assembly that can be removed from the pressure housing. Additional coils are installed to indicate the top and bottom limit positions to permit detection of those limits. FSAR Tier 2, Revision 2, Section 4.6.1, states that the CRDMs are equipped with a digital and analog position indication system to measure control rod position over the height of the core by two diverse methods:

- A digital measurement that is non-safety-related
- An analog measurement, based on position indicator coils, that is safety-related

FSAR Tier 2, Section 7.1.1.5.14, Interim Revision 3 mark-ups, states that the rod position sensor is comprised of one primary and three secondary coils (as discussed in FSAR Tier 2, Figure 7.1-25, Interim Revision 3 mark-ups). Two of the secondary coils, called auxiliary secondary coils, indicate the rod at its lowest or highest end position. The third secondary coil, or main secondary coil, indicates the entire range of rod travel. The analog position measurement of the RPMS is derived from the magnetic coupling through the control rod between the primary coil and the secondary coils. The auxiliary secondary coil signal determines the extreme positions of the drive rod. The RPMS receives four inputs from the CRDM, which are the rod top signal, analog rod position signal, rod bottom signal, and temperature measurement signal for compensation. The RPMS conditions these signals, and performs temperature compensation of the analog rod position measurement. The signal processing is performed by analog conditioning modules and a TXS processing unit, the rod position measurement unit. The RPMS provides three signal outputs that include top, bottom,

and temperature compensated analog position. The RPMS sends the control rod position measurement signals to the SCDS. The SCDS sends the rod position and measurement signals to the RCSL. The PICS interfaces with the RCSL system to provide the operator with control and monitoring capability of the core control functions. Additionally, FSAR Tier 2, Revision 2, Section 4.6.1, states that a safety-related rod position limit sensor provides input to the PS when the rod is at the bottom position and a non-safety-related upper position limit sensor provides indication when the rod is at the top position.

FSAR Tier 2, Revision 2, Section 4.6.1, states that the digital measurement counts CRDM movement steps to provide a digital measurement of control rod position. FSAR Tier 2, Section 7.7.1.1 states that this signal is called a feedback signal which travels from the CRDCS rod control unit to the RCSL system and provides information for digital position indication of the control rods based on the number of rod movement steps sent to the control rods. This digital control is then sent from the RCSL to the PICS for display in the MCR. This control rod position measurement is used by the operators in the MCR to compare with rod position indications provided by the RPMS rod position signals that are displayed in the MCR.

When power is interrupted to the control rod operating coils, the CRDM releases the control rods and the rods are inserted into the core by gravity. FSAR Tier 2, Revision 2, Section 4.6.2, states that this power supply to the coils of the control rods is classified as non-safety related.

FSAR Tier 2, Table 7.1-2, Interim Revision 3 mark-ups, identifies that the CRDCS will be designed to the applicable regulatory criterion of GDC 13 and GDC 19. The staff finds that the CRDCS provides adequate instrumentation to control and monitor control rod movements and position. In addition, the staff also finds that the CRDCS is appropriate for executing requested rod movement commands received from the RCSL. Accordingly, the staff finds that the CRDCS meets the applicable regulatory criterion of GDC 13 and GDC 19.

#### *7.7.4.3.3 Process Automation System Design Bases Evaluation*

##### *7.7.4.3.3.1 Maintaining Plant Variables within Predefined and Allowable Ranges*

10 CFR Part 50, Appendix A, GDC 10, "Reactor Design," requires that the reactor core and associated coolant, control, and protection systems be designed with appropriate margin to assure that specified fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. 10 CFR Part 50, Appendix A, GDC 15, "RCS Design," requires that the RCS and associated auxiliary, control, and protection system be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences. The staff used the guidance of SRP Section 7.7 to evaluate the applicant's design descriptions for conformance to the regulations.

The PAS performs the plant control functions listed in Table 7.7-3 below. Not all PAS plant functions are listed within the table. However, the table represents the major non-safety related I&C control functions that will be used during normal plant operation and mitigation of postulated AOOs. These functions are designed to act before the protection function setpoints to maintain and/or restore normal plant operating conditions without challenging the safety-related protective actuations. The PAS control function thresholds for actuation are set to actuate before the safety-related PS setpoints, keeping the monitored plant parameter within a defined operating range.

**Table 7.7-3 PAS Major Control Functions<sup>3</sup>**

<b>Plant Variable Monitored</b>	<b>PAS Generates Signals to</b>	<b>Design Basis</b>
RCS pressure control	Actuate pressurizer (PRZ) heaters or normal spray.	Maintains the RCS pressure within allowable limits
PRZ level control	Actuates control valves in the CVCS letdown lines	Maintain the pressurizer level within the allowable range
RCS loop level control	Control coolant letdown flowrate.	Control RCS water inventory during mid-loop operation.
SG (SG) level control	Control valves in the main feedwater system (MFWS)	Maintain SG level automatically
Main steam (MS) pressure control	Automatically modulate turbine bypass valves	Provide MS overpressure control
Residual heat removal system function	Deenergize pressurizer heaters and actuate normal spray	Protects the RHRS from over pressurization and opening PZR safety relief valves
Reactor coolant pump function	Secures the pressurizer spray and energizes pressurizer heaters	Avoids a RT on Min2p (i.e., low PZR pressure) during Mode 1
Reactor pressure vessel brittle fracture function	Stops the CVCS charging pumps, the medium head safety injection (MHSI) pumps, the extra borating system pumps, and de-energizes the PZR heaters.	Prevent pressure from reaching the PRZ safety relief valve open setpoints when in Mode 4 and Mode 5

As an example of PAS plant control functions, the PAS provides automatic RCS pressure control and automatic pressurizer level control. The RCS pressure control maintains pressure within allowable limits during Mode 1 through Mode 5. When in the automatic pressure control mode, the pressure control maintains the primary pressure at a setpoint value in steady-state operation and within an allowable range around its setpoint (i.e., control band) during transients, including startup and cooldown operations. RCS pressure control is performed by actuating pressurizer heaters or normal spray. The pressurizer level control provides:

- Sufficient RCS water inventory for cooling and for proper control of RCS pressure
- A sufficient steam volume in the pressurizer to accommodate in-surges in the pressurizer from the RCS without causing an excessive pressure increase for normal operating transients

---

<sup>3</sup> Created from design descriptions contained in FSAR Tier 2, Section 7.7, "Control Systems Not Required for Safety," Interim Revision 3 mark-ups.

The pressurizer level control monitors level for deviations from its setpoint during Mode 1 through Mode 4, and based on mode changes, actuates different control valves at the reducing stations located in the chemical and volume control system letdown lines. FSAR Tier 2, Figures 7.7-3 and 7.7-4, Interim Revision 3, illustrate the pressurizer pressure and level control bands.

As another example, the PAS automatically maintains SG level by matching feedwater flow to steam demand. During normal operations, the PAS operates the below listed main feedwater system valves in order to control and maintain SG level within the control band:

- Full load control valve
- Low load control valve
- Very low load control valve

FSAR Tier 2, Figure 7.7-5, Interim Revision 3, illustrates the SG level control bands. The PAS actuates the above listed feedwater valves to maintain the SG level within the control band (represented as horizontal dashed lines on FSAR Tier 2, Figure 7.7-5). The program band provides margin for the SG level control programming to accommodate plant transients and plant responses to normal load changes and anticipated operational occurrences. This example for SG level control by PAS is similar to other operating plant control functions controlled by the PAS.

FSAR Tier 2, Table 7.1-2, Interim Revision 3 mark-ups, indicate that the PAS will be design to the applicable requirements of GDC 10 and GDC 15. As illustrated in the above examples, and based on the design descriptions in FSAR Tier 2, the staff concludes that the PAS is designed with appropriate and sufficient margin to assure that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences. Accordingly, the staff concludes that the PAS meets the applicable requirements of GDC 10 and GDC 15.

#### 7.7.4.3.3.2 Instrumentation to Monitor and Control Plant Variables and Systems

GDC 13, "Instrumentation and Control," requires that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. GDC 19, "Control Room," requires, among other things, that equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

The staff used the guidance contained in SRP Section 7.7 to evaluate the applicant's design descriptions for conformance to the Commission's regulations. SRP Section 7.7 states that the review should confirm that the control systems include the necessary features for manual and automatic control of process variables within prescribed normal operating limits. It also states that the review should confirm that I&C systems include environmental control as necessary to protect equipment from environmental extremes.



The PAS CUs are connected to the PICS to receive manual commands generated from the PICS in the MCR and to display measured plant parameters on the PICS in the MCR. The operator is able to manually control the PAS system components by using the PICS control system located within the MCR. Operator commands from the PICS for component level control of safety-related process systems are actuated by the PAS. The operator performs the manual command from the PICS, the PICS sends the command signal to the PAS and the PAS sends the component actuation signal to the PACS. The operator has the ability to place the PAS functions in an automatic control mode or in a manual control mode. The operator performs the mode selection from the PICS from the MCR. PAS utilizes redundant CUs to perform its functions. The CUs acquire hardwired signals from the SCDS, DAS, PS, SAS, field sensors, and/or black boxes. Outputs are sent to non-safety-related actuators directly or to the PACS. Interfaces are also provided with the TG I&C system. The CUs interface with the PICS for manual commands and display of information.

FSAR Tier 2, Table 7.1-2, Interim Revision 3 mark-ups, indicate that the PAS will be designed to meet the requirements of GDC 13 and GDC 19. The staff finds that PAS contains the necessary instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions as appropriate and is capable of maintaining system variables within predefined operating ranges and that PAS allows the operator to take necessary actions from the MCR to operate the plant safely during normal operation, including anticipated operational occurrences. Accordingly, the staff finds that PAS meets the requirements of GDC 13 and GDC 19.

#### *7.7.4.3.4 Process Information and Control System Design Bases Evaluation*

Since PICS is a non-safety-related display, system annunciator, and operator control system, it was not evaluated for conformance to GDC 10 and GDC 15, as these requirements are not applicable to this system. The PICS was evaluated for conformance to requirements GDC 13 and GDC 19. GDC 13, "Instrumentation and Control," requires that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. GDC 19, "Control Room," requires, among other things, that equipment at appropriate locations outside the control room be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. The staff used the guidance contained in SRP Section 7.7 to evaluate the applicant's design descriptions for conformance to the Commission's regulations. SRP Section 7.7 states that the review should confirm that the control systems include the necessary features for manual and automatic control of process variables within prescribed normal operating limits. It also states that the review should confirm that I&C systems include environmental control as necessary to protect equipment from environmental extremes.

FSAR Tier 2, Section 7.1.1.3.2, Interim Revision 3 mark-ups, states that the PICS is intended to be used during normal, accident, and severe accident conditions as long as it is available. PICS is designed to control both safety-related and non-safety-related equipment. PICS equipment is located in Safeguard Buildings that provide a mild environment during and following AOOs or PAs. FSAR Tier 2, Figure 7.1-2, Interim Revision 3, provides the PICS architecture. Redundant

gateways are provided for communication with the PS, SAS, RCSL, and the turbine-generator I&C system. PICS receives uni-directional signals from the PS and SAS to obtain status information on those systems. PICS communicates bi-directionally with the RCSL and TG I&C system. Redundant servers are provided so that the PICS remains operational in case of a failure of a single server. The PICS is able to transmit data through a firewall to systems external to the plant I&C system. The redundant servers and redundant segments of the automation busses are physically located in separate fire areas so that a fire in the MCR does not result in a loss of the PICS to the remote shutdown station.

The staff's evaluation regarding the capability of PICS to monitor plant variables is discussed in Section 7.5 of this report. The staff finds that the PICS design addresses the applicable guidance of SRP Section 7.7 since PICS provides the capability for monitoring variables, including post-accident monitoring variables and system variables over their anticipated ranges for normal operation, for anticipated operational occurrences, and for postulated accidents. PICS also provide a means of manual control capabilities for maintaining plant variables and systems within prescribed operating ranges. Accordingly, the staff finds that PICS conforms to the applicable requirements of GDCs 13 and 19.

#### 7.7.4.4 *Control System Failure Analysis Evaluation*

GDC 28, "Reactivity Limits," requires that the reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly the capability to cool the core. GDC 29, "Protection Against Anticipated Operational Occurrences," requires that the protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences. The staff used the guidance of SRP Section 7.7 to evaluate the applicant's design descriptions for conformance to the agency's regulations.

The RCSL contains the control logic to maintain or bring reactor core parameters back into their defined normal operating ranges, before reaching a safety-related protective system setpoint, by initiating functions to:

- block rod withdrawal or insertion
- increase or decrease control rod movement speed
- block or start boron addition or dilution

The CRDCS rod control units generate the input to the corresponding CRDCS coil modules in order to control the rod speed and movement for one control rod. The coil modules control the amount of current applied to the operating coils (i.e., lift coil, movable gripper coil and stationery gripper coil) of the CRDM in order to move the corresponding control rod. FSAR Tier 1, Table 2.4.13-3, ITAAC Item 4.4 Interim Revision 3 mark-ups, , verifies that the CRDCS limits the RCCA bank withdrawal rate to 76.2 cm/minute (30 in./minute) or less. Therefore, the staff finds that appropriate limits have been placed on reactivity increases and that control rod reactivity addition limits (i.e., control rod withdrawal speed) as part of the design.

FSAR Tier 2, Revision 2, Section 15.0.0.3.6, states that when considering plant systems and components available for mitigation of accident analysis, non-safety-related control systems are simulated when their operation makes the response of the event more severe. In this case, it is assumed that they function as designed and failures of the non-safety related control systems are considered only as event initiators.

RCSL equipment divisions are physically separated from one another and are electrically isolated from each other. Therefore, a failure from one division will not propagate to other divisions and the failure of a function in one division is backed up by a redundant function in another division.

Control functions are separated between the RCSL and the PAS system. Functions related to reactor core power control are assigned to the RCSL system and plant control functions related to RCS are assigned to the PAS. Failures of components in one of these non-safety systems (i.e., PAS) do not affect the functioning of the other non-safety related system (i.e., RCSL). RCSL and PAS setpoint actuations act before safety-related PS setpoint actuations. Therefore, the RCSL and PAS actuations will keep or return plant disturbances to the normal operating range before reaching a safety-related actuation threshold. Functions assigned to RCSL and PAS are redundant in more than one division. The failure of a function in one division is backed up by a redundant function in another division. The redundant functions and their associated equipment, including support systems are independent of each other. Design attributes that protect against non-safety related control system failures include:

- Redundant functions are allocated to physically separated divisions
- Electrical isolation between divisions
- Erroneous signals or messages from one faulty division do not impair the functionality of the remaining divisions

The primary source of power to the RCSL and PAS is the 12-hour uninterruptible power supply and the station black out diesel generators. The secondary power source is the turbine building's non-Class 1E uninterruptible power supply, which is fed from a different power bus. The same power supply provides backup power with 2-hour batteries and the station blackout diesel generators in the event of a loss-of-offsite power. Upon loss of the primary source of power to PAS or RCSL, the secondary power source automatically and without interruption, maintains power. In the case of a total loss of power to the plant, the battery source permits continued operation of the plant controls for a two-hour period. The CRDCS receives DC power from the non-Class 1E uninterruptible power supply to move and hold the CRDMs. The non-safety-related components of the CRDCS are designed such that a seismic event does not result in damage that disables the safety function of the RT contactors.

To help reduce potential failure modes for non-safety-related control systems, environmental controls are provided to protect equipment from environmental extremes. HVAC is provided to maintain ambient conditions in a range acceptable for proper operation of I&C equipment.

The staff reviewed the plant's accident analysis descriptions located in FSAR Tier 2, Revision 2, Section 15, to determine whether reactivity control system failures (i.e. AOOs) were bounded by safety-related system thresholds. For postulated AOOs of control system, increases in reactor power would cause a reactor scram initiated by the PS on events that would lead a full reactor scram due to either a high neutron flux rate of change, high pressurizer level, low departure from nucleate boiling ratio, high linear power distribution, high core power level, or high SG

pressure protection system threshold being exceeded. Therefore, the staff confirmed that the consequential effects of AOOs do not result in reactivity control system failures that would cause plant conditions more severe than those bounded by the analysis of the events. Accordingly, the staff concludes that functional requirements for reactivity control systems have been provided to limit reactivity increases to prevent or limit the effect of reactivity accidents. Based on this finding, the staff finds that the applicable requirements of GDC 28 have been met for the reactivity control systems. Based on the above design features, the staff concludes that the reactivity control systems have been designed to assure an extremely high probability of accomplishing their functions in the event of anticipated operational occurrences. Accordingly, the staff finds that the applicable requirements of GDC 29 have been met for the reactivity control systems.

#### **7.7.5 Combined License Information Items**

FSAR Tier 2, Section 7.7.2.3.5, Interim Revision 3 mark-ups, states that a COL applicant that references the U.S. EPR design certification will, following selection of the actual plant operating instrumentation and calculation of the instrumentation uncertainties of the operating plant parameters, prior to fuel load, calculates the primary power calorimetric uncertainty. The calculations will be completed using an NRC acceptable method and confirm that the safety analysis primary power calorimetric uncertainty bounds the calculated values. The staff finds inclusion of the COL Information Item to be appropriate to address secondary calorimetric uncertainty.

#### **7.7.6 Findings and Conclusions**

With the exception of the open item identified in this section, the staff concludes that the design of the control systems is acceptable and meets the relevant requirements of GDC 1, GDC 10, GDC 13, GDC 15, GDC 19, GDC 24, GDC 28, and GDC 29, and of 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h) once the applicant has satisfactorily addressed open item RAI 505, Question 07.07-23 identified within Section 7.7.4.2 of the report.

The staff conducted a review of the control systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these control systems. The staff concluded that the applicant adequately classified and identified the guidelines applicable to these systems. The staff finds that the control systems are appropriately designed and are of sufficient quality to minimize the potential for challenges to safety systems. However, one open item was identified regarding the commitment for PICS equipment qualification, as described in Section 7.7.4.2.4 of this report. Based upon the review of the system design, the staff finds that once the RAI 505, Question 07.07-23, identified within Section 7.7.4.2 of the report for PICS equipment qualification has been satisfactorily resolved, the staff will have reasonable assurance that the systems conform to the requirements of GDC 1 and 10 CFR 50.55a(a)(1).

The staff conducted a review of the plant transient response to normal load changes and anticipated operational occurrences such as reactor trip, turbine trip, upsets in the feedwater, and steam bypass systems. The staff concludes that the control systems are capable of maintaining system variables within prescribed operating ranges. Therefore, the staff finds that the control systems satisfy this aspect of the requirements of GDC 13.

The staff's review of the control systems considered the features of these systems for both manual and automatic control of the process systems. The staff finds that the features for

manual and automatic control facilitate the capability to maintain plant variables within prescribed operating limits. The staff also finds that the control systems permit appropriate actions to be taken to operate the plant safely during normal operation and AOOs and accidents, from the MCR. Therefore, the staff finds that the control systems satisfy the requirements of GDC 19 with regard to normal plant operations.

The staff concludes that the design of the control systems is acceptable and meets the applicable requirements of GDC 10 and GDC 15.

The conclusions of the analysis of anticipated operational occurrences and postulated accidents as presented in FSAR Tier 2, Chapter 15 been used to confirm that plant safety is not dependent upon the response of the control systems. The staff also confirmed that failure of the control systems themselves or as a consequence of supporting system failures, such as loss of power sources, does not result in plant conditions more severe than those described in the analysis of design basis accidents and anticipated operational occurrences. The staff confirmed that the consequential effects of AOOs and postulated accidents do not result in control system failures that would cause plant conditions more severe than those bounded by the analysis of the events. The staff finds that the applicable requirements of GDC 28 and GDC 29 have been met for the control system design.

The staff confirmed that the control systems design and performance information and the level of detail in FSAR Tier 1 are commensurate with the safety significance of the control systems credited functionality for the design. FSAR Tier 1 information includes the principal performance characteristics of the control systems and will be verified appropriately by ITAAC. The staff confirmed that FSAR Tier 1 ITAAC acceptance criteria compliance is verifiable through ITAAC and the method to be used for verification is adequate. Therefore, the staff finds that the non-safety-related control system FSAR Tier 1 design information contains the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act of 1954 (as amended), and NRC regulations, and thus, conforms to the applicable ITAAC requirements of 10 CFR 52.47(b)(1).

## **7.8 Diverse I&C Systems**

### **7.8.1 Introduction**

Diversity of the I&C systems is described in FSAR Tier 2, Section 7.8, and Technical Report ANP-10304, "U.S. EPR Diversity and Defense-in-Depth Assessment," Revision 4. The design information in these documents consists of:

- The defense-in-depth and diversity (D3) design for the U.S. EPR I&C systems.
- The design features that prevent and mitigate a SCCF of the safety I&C systems.
- The design features to address an anticipated transient without scram (ATWS).
- A methodology to evaluate the D3 aspects of the I&C architecture to determine if the I&C system will adequately protect the health and safety of the public in the unlikely event of an SCCF.

## 7.8.2 Summary of Application

**FSAR Tier 1:** The FSAR Tier 1 information associated with this section is found in FSAR Tier 1, Section 2.4.2, “Safety Information and Control System,” Section 2.4.4, “Safety Automation System,” Section 2.4.5, “Priority Actuator and Control System,” Section 2.4.24, “Diverse Actuation System,” and Section 2.4.25, “Signal Conditioning and Distribution System.”

**FSAR Tier 2:** The applicant provided a system description of the defense-in-depth and diversity analysis FSAR Tier 2, Section 7.8, which is summarized in the following discussion.

The DAS executes the automatic reactor trip, ESF actuation, and alarm and display functions to address the potential for an SCCF and an ATWS. The DAS is a diverse I&C system from the safety-related I&C systems (PS and SAS). Sensor information is acquired by the DAS from the SCDS using a hardwired signal that is electrically isolated within the safety I&C systems and is not affected by a SCCF. These functions are set so that the PS will actuate prior to the DAS. For reactor trip functions, outputs from the DAS are sent to the shunt trip coils of the reactor trip breakers, which are a diverse means of opening the breakers from the under-voltage coils which are actuated by the PS. For ESF functions, outputs from the DAS bypass the PS and SAS and are sent directly to the PACS. Outputs for turbine trip are sent directly to the TG I&C. Alarms and indications are processed by the DAS and are sent to PICS and SICS for display. SICS is a hardwired human-machine interface that is not susceptible to a SCCF and provides the system-level and component-level manual actions that may be needed to address an SCCF.

In the event of a SCCF, manual and automatic commands are initiated from the SICS and DAS, and transmitted to the PACS for signal prioritization and actuation of plant components. This path allows the actuation and control of safety systems by the operator in the event of a SCCF of the safety I&C systems. PACS is credited as being diverse in operation from the TXS platform used in the PS and SAS. In addition, the PACS safety logic will be verified by 100 percent combinatorial testing. The PACS is not used in the actuation path for the RT function.

**ITAAC:** The ITAAC associated with FSAR Tier 2, Section 7.8 are given in FSAR Tier 1, Table 2.4.2-2 — Safety Information and Control System ITAAC, Table 2.4.5-2 — Priority Actuator and Control System ITAAC, and Table 2.4.24-4 — Diverse Actuation System ITAAC.

**Technical Specifications:** There are no Technical Specifications associated with FSAR Tier 2, Section 7.8.

## 7.8.3 Regulatory Basis

The design of diverse I&C systems shall meet the relevant requirements of the following Commission regulations:

1. GDC 13, “Instrumentation and Control,” as it relates to assuring Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems
2. GDC 19, “Control Room,” as it relates to providing a control room from which actions can be taken to operate the nuclear power unit safely under normal conditions and to

maintain it in a safe condition under accident conditions, including loss-of-coolant accidents

3. GDC 22, "Protection System Independence," as it relates to the design of the protection system to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function.
4. GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.
5. 10 CFR 50, Appendix A, GDC 1, "Quality Standards and Records"
6. 10 CFR 50.55a(a)(1), "Quality Standards"
7. 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Std 603-1991. For diverse actuation systems isolated from safety systems, the applicable requirements of 10 CFR 50.55a(h) are IEEE Std 603-1991, Clause 6.3, "Interaction Between the Sense and Command Features and Other Systems"
8. 10 CFR 50.62, "Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants."
9. 10 CFR 52.47(b)(1), "Contents of applications; technical information," requires that a design certification contain the proposed inspections, tests, analyses, and acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act of 1954, and NRC regulations.

#### **7.8.4 Technical Evaluation**

The objectives of this review are to assure that the ATWS mitigation systems and equipment are designed and installed in accordance with the requirements of 10 CFR 50.62, and that other diverse I&C systems within the scope of this section comply with NRC policy on D3 for digital I&C systems. Specifically, the staff verified the following for the U.S. EPR design:

- Adequate D3 has been provided in the design to meet NRC requirements.
- Verify that the displays and manual controls for critical safety functions initiated by operator action are diverse from those that are available on the computer systems used in the automatic portion of the protection systems.

Several other design considerations are addressed in other Sections of this report, as indicated in Table 7.8-1 below.

**Table 7.8-1 Design Considerations Referenced in Other Sections of this Report.**

<b>Design Considerations</b>	<b>Report Section(s)</b>
10 CFR 50.55a(a)(3)	7.1.4.1
Quality Standards and Records, 10 CFR 50.55a(a)(1), GDC1	7.1.4.10, 7.1.4.13
Control Room, GDC 19	7.5.4
10 CFR 50.55a(h)(3), GDC 12 and GDC 24,”	7.1.3.12.3, 7.1.4.12.4

10 CFR 50.55a(a)(3) allows applicants under 10 CFR Part 52, to propose alternatives to the requirements of 10 CFR 50.55a(h)(3) or portions thereof. The U.S. EPR design certification applicant proposes to use IEEE Std 603-1998 as an alternative to 10 CFR 50.55a(h)(3) which requires the use of IEEE Std 603-1991. Section 7.1.4.1 of this report discusses the staff evaluation and approval of this alternative. IEEE Std 603-1998 introduces a new clause that is not found in IEEE Std 603-1991 version. Specifically, Clause 5.16, “Common cause failure criteria,” requires, in part, that plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure. This section of the report will address how the applicant met this requirement.

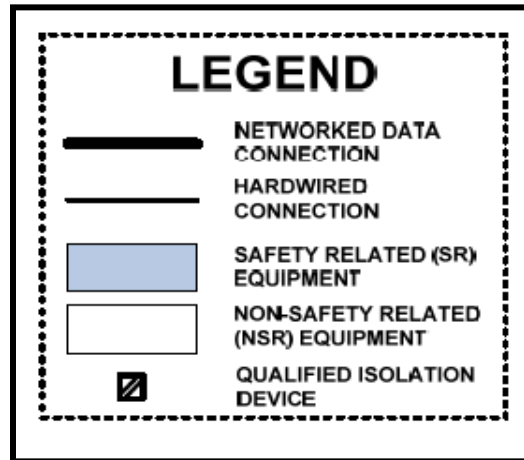
At the time of the staff’s review, FSAR, Revision 2 was the latest docketed version of the application. However, in response to various RAI, the applicant provided Interim Revision 3 mark-ups, that the staff used in preparing this report. Regarding the information in FSAR Tier 2, Section 7.8, the applicant provided Interim Revision 3 mark-ups for this section in a May 25, 2011, response to RAI 413, Question 07.08-13. In a June 22, 2011, response to RAI 452, Question 07.03-36, the applicant provided Interim Revision 3 mark-ups for FSAR Tier 1, Section 2.4. Upon receipt of the final Revision 3 of the FSAR, the staff will verify incorporation of the Interim Revision 3 mark-ups. **RAI 413, Question 07.08-13 and RAI 452, Question 07.03-36 are being tracked as confirmatory items.** The staff used the guidance listed below to assess the adequacy of U.S. EPR D3 I&C design diversity and to evaluate conformance to the applicable regulatory criteria:

- NUREG-0800, Section 7.8, “Standard Review Plan,” Revision 5, March 2007
- SRP BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” Revision 5, March 2007
- The Staff Requirements Memorandum to of SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," Item II.Q
- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994
- Digital Instrumentation and Controls Task Working Group #2: “Diversity and Defense-in-Depth Issues,” Interim Staff Guidance (ISG-02), Revision 2, June 2009
- Digital Instrumentation and Controls Task Working Group No. 4, “Highly Integrated Control Room – Communications, Revision 1



- NUREG-0800, Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses, Revision 0, November 2009
- NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, January 2004
- Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," and its enclosure, April 1985

The below legend is applicable for all figures listed in this section of this report.



**Figure 7.8-1 Legend Applicable to all figures of this section**

#### 7.8.4.1 *Diversity Between U.S. EPR I&C Systems*

##### 7.8.4.1.1 *Anticipated Transient Without Scram Diversity Evaluation*

10 CFR 50.62 requires, in part, that each pressurized water reactor must have equipment from sensor output to final actuation device that is diverse from the reactor trip system (RTS) to automatically initiate the auxiliary (or emergency) feedwater system and to initiate a turbine trip under conditions indicative of an ATWS, and for certain cases, requires a diverse scram system from the sensor output to interruption of power to the control rods.

FSAR Tier 1, Section 2.4.24, Interim Revision 3 mark-ups, states that the DAS is a non-safety-related digital I&C system that provides mitigation against AOOs or PAs concurrent with an SCCF of the PS. FSAR Tier 2, Section 7.8.1.1.3, Interim Revision 3 mark-ups, states that DAS executes automatic functions to mitigate an ATWS and that DAS is diverse from PS. FSAR Tier 2, Revision 2, Section 15.8.1.3, "Diverse Actuation System," states DAS contains the logic to address ATWS requirements of 10 CFR 50.62, that DAS is independent from sensor output to the final actuation device from the PS, and DAS provides a diverse method to trip the reactor, trip the turbine, and initiate the EFW system on conditions indicative of an ATWS. These diverse functions provided by the DAS are credited by the applicant to provide reasonable assurance that a pressure increase does not exceed the ASME Service Level C limit of 3,200 psig and does not exceed containment safety parameters. Technical Report ANP-10304, Section 3.2, states that DAS automatically initiates reactor trip and ESF to mitigate a postulated SCCF of the PS that prevents the PS from mitigating an AOO or PA. Technical Report ANP-10304, Section A.1 also states that the ATWS mitigation system for the

U.S. EPR is the DAS. Therefore, staff finds DAS is the credited I&C system that provides the ATWS mitigation function required by 10 CFR 50.62. The staff used the diversity analysis guidance in NUREG/CR-6303 to evaluate the diversity of the DAS as compared to the PS. The diversity categories in NUREG/CR-6303 are:

- design diversity
- equipment diversity
- functional diversity
- human diversity
- signal diversity
- software diversity

Design diversity is as the use of different approaches, including software and hardware, to solve the same, or a similar, problem. The focus for this diversity category is on technology, approach, and architectural differences. Essentially, the design diversity attribute relates to technology choice and usage. This diversity category has three diversity attributes (listed in order of effectiveness) that contribute to diversity between two designs that meet the same or similar requirements:

- different technologies (e.g., analog versus digital)
- different approaches within the same technology (e.g., transformer-coupled AC instrumentation versus DC-coupled instrumentation)
- different architecture (i.e., arrangement and connection of components)

Technical Report ANP-10304, Revision 4, Section 2.2 states that the DAS will be implemented with either electrical, electronic, or programmable electronic technology that is not microprocessor based. FSAR Tier 2, Section 7.1.1.4.1, Interim Revision 3 mark-ups, identifies the PS as being implemented with the TXS platform, which is microprocessor-based system. The approach to design a platform with a microprocessor is different than a system without a microprocessor. Technical Report ANP-10304 Section 4.2 states the DAS architecture shown in FSAR Tier 2, Section 7.1, is different from the PS architecture. The staff's review of the PS architecture in FSAR Tier 2, Figure 7.1-6, and the DAS architecture in FSAR Tier 2, Figure 7.1-13, did not reveal the internal arrangement of components for the DAS. However, Technical Report ANP-10304, Section 3.2.1 provides a design commitment that "the design architecture will be different" between the DAS and the TXS platform used to implement the PS. Therefore, based on the documented design commitments, staff approves the design diversity attributes of "different approaches within the same technology" and "different architecture" between the DAS and the PS.

Equipment diversity is the use of different equipment to perform similar safety functions, in which "different" means sufficiently unlike as to significantly decrease vulnerability to common failure. These diversity attributes for this diversity type, in order of effectiveness, are:

- different manufacturers of fundamentally different designs

- same manufacturer of fundamentally different designs
- different manufacturers making the same design
- different versions of the same design

Technical Report ANP-10304, Revision 4, Section 2.2 states that the DAS will be implemented with either electrical, electronic, or a non-microprocessor-based I&C platform, while the PS is implemented with the microprocessor-based TXS platform. Technical Report ANP-10304, Section 3.2.1 states that the power supplies will be from different manufacturers. FSAR Tier 2, Sections 7.2.2.3.4 and 7.3.2.3.5, Interim Revision 3 mark-ups, provides a design commitment that technology used in the DAS is diverse from the technology used in the PS. However, the staff was not able to locate a design commitment in FSAR Tier 2, Section 7 or Technical Report ANP-10304 that provides a design commitment that the DAS system and/or components would be developed using a different manufacturer than the PS components and equipment. Therefore, the staff did not credit any diversity attributes using different manufacturers for the DAS and PS. Staff did approve the equipment diversity attribute of same manufacturer of fundamentally different designs.

Equipment diversity acknowledges the features that contribute to diversity in the equipment essential to providing logic processing of functions. The focus for these criteria under the general "equipment" diversity attribute is on the type of logic processing equipment employed. These diversity attributes for this diversity type, in order of effectiveness, are:

- different logic processing equipment architecture
- different logic processing version in the same architecture
- different component integration architecture
- different data-flow architecture

Technical Report ANP-10304, Section 4.2 states that the DAS will not be microprocessor-based, whereas the PS utilizes function processors. This difference in selected technology between the DAS and the PS provides for different logic processing between the equipment for the DAS and the TXS equipment for the PS. In addition, this difference in selected technology will require a different equipment architecture implementation and different component integration. In addition, this technology difference would provide for different data flow characteristics. Therefore, the staff credited the logic processing equipment diversity attributes of different logic processing equipment for DAS and PS diversity.

Functional diversity states that two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. For example, cooling systems normally intended to function when containment is isolated are functionally different from other liquid control systems intended to inject coolant or borated water for other reasons. Three diversity attribute criteria (listed in decreasing order of effectiveness) that contribute to the diversity of functions between two independent systems, are:

- different underlying mechanisms
- different purpose, function, control logic, or actuation means

- different response time scale

The PS and the DAS perform similar functions for accident mitigation. As stated in FSAR Tier 2, Section 7.1.1.6.5, Interim Revision 3 mark-ups, the DAS is a functional substitute to the PS. However, the DAS performs its functions on a different response time scale and utilizes different actuation means. FSAR Tier 2, Section 7.8.1.1.3, Interim Revision 3 mark-ups, and Technical Report ANP-10304, Section 3.22.1 state that for reactor trip functions, the PS output signal to the reactor trip contactors is de-energized to actuate dropping the control rods while the DAS output signal to the rod control units of the CRDS is energized to actuate dropping the control rods. This diverse actuation means constitutes a different actuation means and/or control logic for performing a reactor trip between the DAS and the PS output signals. Technical Report ANP-10304, Section 4.2 states that the DAS is designed with the intent of allowing the PS to actuate before the DAS, in response to a design basis event. The staff reviewed Technical Report ANP-10304, Table A.2.3 which provides a comparison between the PS and DAS setpoints and time delays. This table demonstrates different accident response setpoints and time scales between DAS and PS. However, upon the staff's review of FSAR Tier 2, Table 7.1-3, Interim Revision 3 mark-ups, the underlying mechanisms for protective plant response mitigation actuations are effectively the same between the DAS and the PS (i.e., reactor trip and ESF actuation to the PACS). Therefore, the staff credited the functional diversity attributes of different purpose, function, control logic, or actuation means and different response time scale.

Human diversity focuses on the life-cycle resources that constitute potential sources of systematic faults. The diversity attributes for this diversity category are:

- different design organizations/companies
- different engineering management teams within the same company
- different design and development teams
- different implementation and testing teams

Technical Report ANP-10304, Section 3.2.1 provides a diversity design commitment between the PS and DAS in that the design organization, management, designers, programmers, and testing engineers will be different. However, Technical Report ANP-10304, Section 4.2 also states that it is "likely" that different design organizations will be responsible for the design of the two systems and that this will not be determined until the detailed design of these systems is in progress. The staff notes that these two design statements from Technical Report ANP-10304, Sections 3.2.1 and 4.2, appear to be conflicting. Since the information provided for the design description, taken alone and in combination, should have one and only one interpretation, in RAI 505, Question 07.08-43, the staff requested that the applicant clarify the statements in Technical Report ANP-10304. **RAI 505, Question 07.08-43 is being tracked as an open item.** The staff only credited the diversity attribute of different design and development teams between the DAS and PS since Technical Report ANP-10304, Section 4.2 only credits the use of different engineers.

Signal diversity defines the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly. The diversity attributes for this diversity category are:

- different reactor or process parameters sensed by different physical effects
- different reactor or process parameters sensed by the same physical effect
- the same reactor or process parameter sensed by a different redundant set of similar sensors

FSAR Tier 2, Section 7.8.1.1.3, Interim Revision 3 mark-ups, state that sensors that are shared by the PS and the DAS are periodically tested as part of the PS testing. The sharing of sensors would not demonstrate the use of different sensed parameters to initiate protective actions between the PS and the DAS. In addition, the applicant does not present a D3 signal diversity design commitment for signal diversity between the PS and the DAS. Therefore, the staff did not credit signal diversity between the DAS and the PS in its independent review.

Software diversity is defined as the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals. For example, use of two separately designed programs to compute when a reactor should be tripped. The diversity attributes for this diversity category are:

- different algorithms, logic, and program architecture
- different timing and/or order of execution
- different operating system
- different computer language

Technical Report ANP-10304, Section 4.2 states that if the DAS uses programmable electronic technology that it will not be microprocessor-based and that the software structure will be fundamentally different. The staff was not able to identify design descriptions that would define the characteristics of “software structure” or would demonstrate the diversity achieved between the PS software attributes and the credited software attributes of the DAS software structure to achieve adequate software diversity. Therefore, in RAI 505, Question 07.08-49, the staff requested that the applicant clarify the credited DAS software structure diversity. **RAI 505, Question 07.08-49 is being tracked as an open item..**

Table 7.8-2 below provides list of diversity attributes that the staff credited between PS and DAS to demonstrate defense against postulated SCCF in the PS.

**Table 7.8-2 PS-DAS Diversity Attributes Credited by the Staff**

Diversity Attributes	DAS-PS Design Diversity
<b>Design</b>	
different approaches within the a technology	YES
different architecture	YES
<b>Equipment</b>	
same manufacturer of fundamentally different designs	YES

Diversity Attributes	DAS-PS Design Diversity
different logic processing equipment architecture	YES
Functional	
different purpose, function, control logic, or actuation means	YES
different response time scale	YES
Human	
different designers, engineers, and/or programmers	YES
Software	
different timing and/or order of execution	YES

For diversity in the reactor trip portion of the PS, FSAR Tier 2, Section 7.8.1.1.3, Interim Revision 3 mark-ups, and Technical Report ANP-10304, Section 3.2.1.1, state that reactor trip outputs from the DAS are sent to the shunt trip coils of the reactor trip breakers, which is a diverse means of opening the breakers from the undervoltage coils which are actuated by the PS. DAS also sends an output to the rod control units of the CRDCS to switch off power to the grippers of the CRDM. This mechanism is a diverse means to trip the control rods as compared to the safety-related trip contactors that are de-energized by the PS. In addition, the DAS initiates EFW and trips the turbine on an indicated ATWS event. Based on the credited diversity attributes and the diverse reactor scram actuation of DAS, and satisfactory resolution of the two above open items, the staff finds that the DAS design meets the diversity requirements of 10CFR 50.62 for automatic emergency feedwater and turbine trip initiation and to interrupt power to the control rods..

#### 7.8.4.1.1.1 Evaluation of I&C System Diversity and Defense-in-Depth Design

GDC 22 requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function. Clause 5.16 of IEEE Std 603-1998 requires, in part, that plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure. The D3 position contained in Item II.Q of the SRM to SECY-93-087, Positions 1, 2, and 3, state that an applicant shall analyze each postulated common-[cause] failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods and demonstrate that there is adequate diversity within the design for each of these events. If a postulated common-[cause] failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-[cause] failure, is required to perform either the same function or a different function. If applicable, the applicant should demonstrate that vulnerabilities to common-[cause] failures have been adequately addressed. NUREG/CR-6303 provides guidance for simplifying the I&C system for SCCF analysis and configuring appropriate I&C systems into blocks and selecting the appropriate I&C block(s) to postulate SCCFs concurrent with AOOs and postulated accidents. Concurrent failure of each set of identical blocks in all divisions should be postulated in turn, and the result of the failure should be documented as a finding of the analysis. Section A.2.2 of Technical Report ANP-

10304 identifies the I&C blocks credited to mitigate against postulated SCCFs. Section A.2.2 of Technical Report ANP-10304 lists the following I&C systems that are available to cope with a postulated SCCF of the PS:

- Diverse Actuation System (DAS)
- Process Automation System (PAS)
- Safety Automation System (SAS)
- Priority and Actuator Control System (PACS)
- Safety Information and Control System (SICS)

The staff used the diversity guidance of NUREG/CR-6303 to evaluate the adequacy of diversity within the I&C design.

FSAR Tier 2, Section 7.1.1.4.1 of the Interim Revision 3 mark-ups, identifies the PS as the safety I&C system that detects plant conditions indicative of AOOs and postulated accidents and actuates the safety-related process systems required to mitigate the event. FSAR Tier 2, Section 7.1.1.4.2, Interim Revision 3 mark-ups, states that the SAS is a safety I&C system that performs automatic safety-related control functions to mitigate the effects of AOOs and PAs, and to reach and maintain safe shutdown. PS is the primary protection system which is postulated to fail due to a SCCF. FSAR Tier 2, Section 7.1.1.4.6, Interim Revision 3 mark-ups, states that the non-safety-related PAS is the main automation and control system for the plant and provides controls for both safety-related and non-safety-related equipment. FSAR Tier 2, Section 7.1.1.3.1, Interim Revision 3 mark-ups, states, in part, that the SICS is provided as a safety-related human machine interface and is designed to provide the operator the necessary inventory of controls and indications for mitigation of AOOs and postulated accidents concurrent with a SCCF of the PS.

NUREG/CR-6303 identifies three SCCF types to postulate. Section 4.11 of Technical Report ANP-10304 states that the U.S. EPR design does not use software-based sensors as inputs to the PS, and therefore, the D3 analysis is performed assuming only the Type 2 postulated SCCF concurrent with AOOs and postulated accidents. The following sections document the staff's review of U.S. EPR I&C design diversity for a postulated SCCF of the primary protection system in order to determine points of vulnerability in the design to a SCCF.

#### Postulated SCCF of the PS

The PS is the primary, safety-related I&C system that detects abnormal plant conditions and actuate safety-related systems required to mitigate AOOs or postulated accidents. The applicant designed the DAS as the diverse means to automatically actuate safety-related systems for postulated SCCF of the PS. Based on the staff's diversity review and findings for conforming to the diversity requirements of 10CFR50.62 between DAS and PS in Section 7.8.4.1.1 of this report, the staff finds that the design diversity between the DAS and the PS address the diversity guidance of NUREG/CR-6303, Guideline 2 and the SRM to SECY-93-087, Position 3.

PAS is credited in several accident scenarios of Technical Report ANP-10304, Appendix A to provide continual plant system control functions that are not affected by a postulated PS SCCF. Technical Report ANP-10304, Section 4.12, states that PAS is credited in the D3 analysis and that that it is in continuous operation. Technical Report ANP-10304, Section 4.1 states that normally operating control functions in PAS, such as pressurizer level control and pressurizer pressure control, continue to operate following a postulated SCCF of the PS. Section 4.1 also states that since the PAS function of partial cooldown relies on a PS output signal, this function is not assumed to be operational in the D3 analysis. The credited PAS functions available for accident mitigation are listed Technical Report ANP-10304, Section A.2.2 and Table 7.8-3 below.

**Table 7.8-3 PAS and SAS Automatic System Control Functions.**

<b>I&amp;C Control System</b>	<b>Function</b>
<b>PAS</b>	Main feedwater flow control
	SG level control
	Pressurizer pressure (heaters and spray)
	Pressurizer level control (chemical volume control system charging and letdown)
	Pressurizer level limitation function to isolate charging on high level
	Pressurizer level limitation function to isolate letdown and start second charging pump on low level
	Turbine load (pressure) control
	Main steam pressure control (turbine bypass)
<b>SAS</b>	EFW flow control (limits flow to a depressurized SG)

FSAR Tier 2, Section 7.1.1.4.6, Interim Revision 3 mark-ups, and Technical Report ANP-10304, Section 2.2 state that the PAS will be implemented with a commercial grade I&C platform that is not the TXS platform.

The design diversity category has three diversity attributes (listed in order of effectiveness) that contribute to diversity between two designs that meet the same or similar requirements:

- different technologies
- different approaches within the same technology
- different architecture

Technical Report ANP-10304, Revision 4, Section 4.2 states that the PAS is redundant within a division and between divisions. Technical Report ANP-10304 also states that the PAS is a single layer system (only a control unit layer) while the PS is a multi-layer system. NUREG/CR-6303 states that the rationale for design diversity is that different designs will have different failure modes and will not be susceptible to the same common influences. A factor that



weakens this argument is that different designs may nonetheless use similar elements or approaches. Upon the staff's review of PS block diagram in FSAR Tier 2, Figure 7.1-6, and the PAS block diagram in FSAR Tier 2, Figures 7.1-11 and 7.1-12 (Interim Revision 3 mark-ups), the arrangement and connection of the system components are different. The PS contains several acquisition and processing units and actuation logic units per division, while the PAS contain only a control unit per division. In addition, the PS and the PAS are not designed to address the same or similar set of requirements. While the applicant did not identify the specific platform and technology to be used in the PAS design, with the design commitment that the PAS system will be implemented with a commercial grade I&C platform that is not part of the TXS platform (i.e., PS), the staff finds that the PAS will consist of a different design than the PS. In addition, the arrangement and connection of the dissimilar components between the PAS and the PS meets the design diversity attribute of "different architecture" between the PAS and the PS. Accordingly, the staff finds the design diversity attribute of different architecture between the PAS and the PS acceptable.

Equipment manufacturer diversity attributes for this diversity type, in order of effectiveness, are:

- different manufacturers of fundamentally different designs
- same manufacturer of fundamentally different designs
- different manufacturers making the same design; and different versions of the same design

Technical Report ANP-10304, Section 4.2 states that PAS equipment is specified to be an industrial control platform other than TXS. However, staff was not able to locate any design commitments that the PAS would be manufactured by a different company or manufacturer than the TXS related PS. Therefore, the staff finds that the PAS achieves the design diversity attribute of same manufacturer of fundamentally different designs.

Logic processing equipment diversity attributes for this diversity type, in order of effectiveness, are:

- different logic processing equipment architecture
- different logic processing version in the same architecture
- different component integration architecture
- different data-flow architecture

Technical Report ANP-10304, Section 4.2 states that the PAS uses different algorithms and logic than the PS because of its different purpose and functions, which are built from standard software blocks that are not TXS software blocks. This diversity commitment between PAS and PS is stated in FSAR Tier 2, Section 7.1.1.4.6, Interim Revision 3 mark-ups, and Technical Report ANP-10304 Section 2.2. Therefore, staff finds the diversity logic processing equipment diversity attribute of different logic processing equipment architecture is achieved for the PAS.

Functional diversity attributes (listed in decreasing order of effectiveness) that contribute to the diversity of functions between two independent systems, are:

- different underlying mechanisms

- different purpose, function, control logic, or actuation means
- different response time scale

NUREG/CR-6303 states that two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. Technical Report ANP-10304, Section 4.2 states that the PAS performs automated control functions to regulate the majority of the plant systems that are different from the purpose of the PS that performs automatic actuation functions specifically designed to respond to AOOs or PAs. The applicant concludes that these the two systems require significantly different application software structures. The staff noted that additional clarity is needed for the software structures of PS and PAS and how they address the diversity guidance of NUREG/CR-6303. **The staff issued RAI 505, Question 07.08-49 to address the issue, which is being tracked as an open item.** The staff reviewed the PAS and PS functional requirements listed in FSAR Tier 2, Table 7.1-3, Sheet 1, Interim Revision 3 mark-ups. The design functionality for the PS has reactor trip and ESF actuation identified for the PS, but not the PAS. Likewise, for plant process control functions, several functional requirements are checked off for the PAS, but none are identified for the PS. The staff finds that the PAS and PS perform different physical plant actuation and control functions and are designed for different plant purposes and are functionally diverse. Therefore, upon satisfactory resolution of the above open item, the staff should be able to find that there is sufficient diversity between the PAS and the PS with regards to functional mechanisms, purpose, logic, actuation means, and response time scale.

Human diversity focuses on the influence to life-cycle resources that constitute potential sources of systematic faults. The diversity attributes for this category are:

- different design organizations/companies
- different engineering management teams within the same company
- different designers, engineers, and programmers
- different implementation and testing teams

Technical Report ANP-10304 Section 4.2 states that only the use of different engineers is credited for PAS diversity from the PS. Therefore, staff finds the human diversity attribute of different design and development teams is achieved for diversity between PAS and PS.

Signal diversity defines the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly. The diversity attributes for this diversity category are:

- different reactor or process parameters sensed by different physical effects
- different reactor or process parameters sensed by the same physical effect
- the same reactor or process parameter sensed by a different redundant set of similar sensors

Technical Report ANP-10304, Section 4.2 states that the PAS and the PS both utilize a small set of sensors even though this shared set of identical inputs would be used for fundamentally

different purposes. NUREG/CR-6303 states that signal diversity is the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly. Signal diversity between systems would provide differences in execution profiles between systems. Different sensors are generally involved in achieving signal diversity. Inputs to the analyzed systems (i.e., the sensed plant parameters) should be sensed by different means to demonstrate signal diversity. This ensures that even if one of the independently sensed plant parameters failed or provided a common triggering event to the system, only one of the I&C accident mitigation systems would be affected. However, due to the sharing of similar sensed parameters between the PAS and the PS, the staff does not find signal diversity between the PAS and the PS.

Software diversity is defined as the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals. For example, use of two separately designed programs to compute when a reactor should be tripped. The diversity attributes for this diversity category are:

- different algorithms, logic, and program architecture
- different timing and/or order of execution
- different runtime environment
- different functional representation

Technical Report ANP-10304, Section 4.2 states that the PAS uses completely different algorithms and logic than the PS. In addition, the PAS is designed to address a different set of plant operational requirements than the PS and the PAS utilizes a different I&C platform than the PS. Therefore, the staff approves the software diversity attribute of different algorithms, logic, and program architecture. Table 7.8-4 below provides a summary of the staff's approved diversity attributes for the PAS.

**Table 7.8-4 Summary of PAS-PS Diversity Attributes Credited by the Staff**

<b>Diversity Attributes</b>	<b>Staff Approved PAS-PS Design Diversity</b>
<b>Design</b>	
different architecture	YES
<b>Equipment</b>	
same manufacturer of fundamentally different designs	YES
different logic processing equipment architecture	YES
<b>Functional</b>	
different underlying mechanisms	YES
different purpose, function, control logic, or actuation means	YES

<b>Diversity Attributes</b>	<b>Staff Approved PAS-PS Design Diversity</b>
different response time scale	YES
Human	
different design and development teams	YES
<b>Signal</b>	
None credited by the staff	NO
Software	
different algorithms, logic, and program architecture	YES

Based on the staff's review of the PS-PAS diversity, the design commitment to use a platform that is not the TXS platform, and the different purpose and functionality of the PAS; the staff finds that the design diversity between the PAS and the PS address the diversity guidance of NUREG/CR-6303, Guideline 2 and the SRM to SECY-93-087, Position 3.

Technical Report ANP-10304, Section 4.2 states that the SAS is a single-layer system (only a control unit layer) while the PS is a multi-layer system (APU, ALU). The staff reviewed and compared FSAR Tier 2, Figure 7.1-7, which is the SAS architecture logic drawing against the PS architecture drawing in FSAR Tier 2, Figure 7.1-6, and concluded that the SAS includes different arrangements and different connections of components within each system's architecture design schemes. Therefore, the staff finds the design diversity attribute of different architecture for the SAS-PS design diversity to be achieved.

Technical Report ANP-10304, Section 4.2 does not credit equipment manufacturer diversity for SAS-PS diversity. In addition, since both the SAS and the PS are implemented with identical TXS system components and software, the staff does not find sufficient equipment manufacturer diversity between SAS and PS.

Technical Report ANP-10304, Section 4.2 does not credit logic processing equipment diversity for the SAS-PS diversity. In addition, since both the SAS and the PS are implemented with identical TXS system components and software, the staff does not find sufficient logic processing equipment diversity between SAS and PS.

Technical Report ANP-10304, Section 4.2 states that SAS performs automated control functions of safety-related plant systems, to regulate those systems during normal operation and PS performs automatic actuation functions specifically designed to respond to AOOs or PAs. It also states that the SAS fulfills a fundamentally different purpose than the PS. NUREG/CR-6303, Section 2.6.4, states that two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. The staff's review of FSAR Tier 2, Table 7.1-3 and 7.1-5, "SAS Automatic Safety Function," Interim Revision 3 mark-ups, finds that a majority of the SAS functions would be based on automatic control logic versus automatic initiation actuation logic, and the allocation of functional requirements between SAS and PS are different. Therefore, staff finds sufficient diversity between SAS and PS with respect to different purpose, function, control logic, or actuation means.

Technical Report ANP-10304, Section 4.2 does not credit human diversity from either different organizations, engineers or likewise. Both the SAS and the PS will be implemented using similar design teams, identical TXS system components, software, and development processes. Therefore, the staff did not find sufficient diversity between SAS and PS with respect to human diversity.

Technical Report ANP-10304, Section 4.2 states that the SAS shares a small set of sensors with the PS and these shared input signals are used for fundamentally different purposes. In addition, the report also states that the functions in SAS that use the same sensors as the PS rely on PS outputs for initiation and are, not credited to mitigate a PS failure in the D3 assessment. Technical Report ANP-10304 credits the signal diversity attribute of “different process parameters.” The guidance of NUREG/CR-6303, Section 2.6.5, states that signal diversity is the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly.

FSAR Tier 2, Revision 2, Section 19.1.4.1.1.3, states that for SAS, which is not modeled in detail in the PRA, is modeled with simple undeveloped events that are combined with sensor inputs that could be shared with the PS to capture dependencies in the PRA model. The staff finds that sharing common sensors between the SAS and the PS creates an environment for the possibility of a SCCF between the SAS and PS, and the staff is not able to eliminate the possibility of a CCF between the SAS and PS based on common sensor inputs (i.e., common triggering events between identical TXS equipment and development processes). Therefore, based on the possible system design and development similarities, identical TXS platform, possible common application layer software logic algorithms and/or execution profiles, common sensor inputs, and possible common automatic actuation and voting functional requirements, the staff does not find sufficient signal diversity between the SAS and PS.

Technical Report ANP-10304, Section 4.2 states that the SAS performs different algorithms and logic than the PS, and that the standard TXS software blocks are configured differently in each system to perform the different algorithms and logical functions. NUREG/CR-6303 states that software (logic) diversity is the use of different programs designed and implemented by different development groups, with different key personnel to accomplish the same safety goals. An example would be the use of two separately designed programs (i.e., one designed by the applicant and another designed independently by sub-contractor/company) to compute when a reactor should be tripped.

NUREG/CR-6303 also states that the goal of software diversity is that different programmers will make different mistakes. However, the design of the identical TXS platform system used by the SAS and the PS does not propose to use different programs, different implementation methods, different development groups, and/or different key personnel. Therefore, the driver for substantial differences in software logic between the SAS and PS would be the required functionality of each system. Technical Report ANP-10304, Section 4.2 states that the SAS fulfills a fundamentally different purpose and performs different types of functions than the PS. However, upon the staff’s review of FSAR Tier 2, Table 7.1-5, “SAS Automatic Safety Function,” the SAS does have automatic actuation functions (i.e., LHSI Valves Actuation, Automatic ESWS Actuation). In addition, FSAR Tier 2, Table 7.1-5 also shows that SAS, for certain functions, will “vote” in a similar format (2 out of 4) as the PS. Therefore, there would be some commonality between the identical TXS application software layer requirements for SAS and PS application layer software development and implementation.

The impact on performance includes differences (or similarities) in logic processing mechanisms and functional interactions that can minimize (or maximize) the potential for faulted states to be triggered concurrently due to commonalities in execution profile. Due to shared commonalities between SAS and PS of identical TXS platforms, shared sensor inputs (common triggers), similar functionality (i.e., similar execution profiles), and similar voting logic, the possibility for a common failure between SAS and PS has not been eliminated. Therefore, the staff does not find sufficient diversity between SAS and PS with respect to logic diversity.

**Table 7.8-5 Summary of SAS-PS Diversity Attributes**

<b>Diversity Attributes</b>	<b>Staff Approved PAS-PS Design Diversity</b>
<b>Design</b>	
different architecture	YES
<b>Equipment Manufacturer</b>	
different equipment manufacturer	NO
<b>Logic Processing Equipment</b>	
different logic processing equipment	NO
<b>Functional</b>	
different purpose, function, control logic, or actuation means	YES
<b>Life-Cycle</b>	
different life-cycle processes	NO
<b>Signal</b>	
different signals used	NO
<b>Logic (Software)</b>	
different logic used	NO

As indicated in table 7.8-5, the staff finds that the SAS is not a significant contributor to the adequacy of credited diversity in the U.S. EPR I&C design to prevent a loss of the protective functions. Therefore, in RAI 512 Question 07.08-50, the staff requested that the applicant provide additional D3 accident mitigation design information for a postulated SAS CCF.

**RAI 512, Question 07.08-50 is being tracked as an open item.**

#### 7.8.4.1.1.2 Summary of Automatic Diverse Means for D3

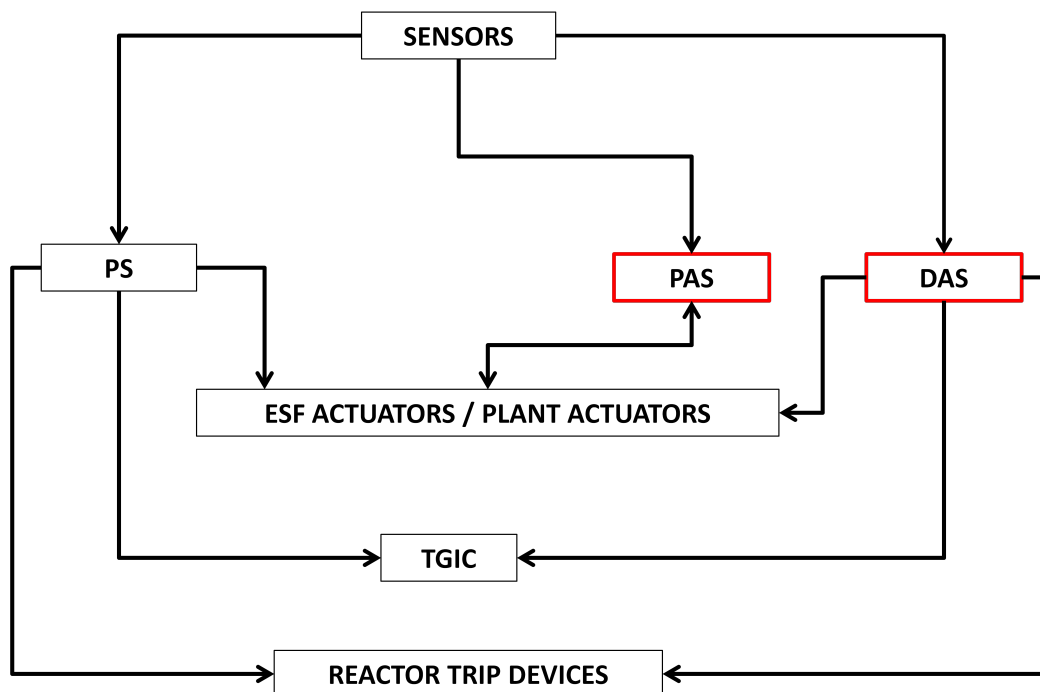
In accordance SRM Item 18, Position 3, to SECY 93-087, the staff finds that the applicant has submitted a documented basis within the Technical Report ANP-10304 that demonstrates that the DAS and SAS provide a diverse means to perform either the same function or a different function for a disabled safety function that was caused by a postulated SCCF to the PS. The documented basis within Technical Report ANP-10304 also demonstrates that the diverse means is unlikely to be subject to the same postulated SCCF as the PS.

Technical Report ANP-10304 Section 2.2 states that the PS utilizes the TXS platform, is a safety-related integrated reactor trip and ESF actuation system, has four redundant, independent divisions, and that each division of the PS contains two independent subsystems to support signal diversity. Section 4.1 of the same report states that I&C systems outside the PS will be used to demonstrate adequate D3 and that signal diversity for reactor trip functions implemented in the PS subsystems are not credited to mitigate any events in the D3 plant response analysis. Accordingly, the staff did not evaluate or include in its evaluation, signal diversity or the automation features of the PS subsystems within its D3 evaluation.

Technical Report ANP-10304, Section 2.2 states that the RCSL performs core-related operational and limitation I&C functions, is non-safety-related, and utilizes the TXS platform. Section 4.1 of the same report states that due to multiple similarities between the PS and RCSL, the RCSL is not credited to terminate events in the D3 assessment. Accordingly, the staff did not evaluate or include the RCSL automation features within this D3 evaluation.

Figure 7.8-2 below displays a block diagram of the automatic D3 mitigation systems that staff credited. Systems with a RED BLOCK (i.e., DAS, PAS) are systems that were credited to provide automatic D3 mitigation actuations and functions. Figure 07.08-2 below does not account for design isolation and/or independence. This figure is only used for demonstrating D3 input and output signal path flow for staff approved automatic D3 mitigation systems. Upon closure of RAI 505, Question 07.08-43 and RAI 512, Question 07.08-50, the staff should be able to find that the U.S. EPR design provides sufficient diversity for automatic D3 functions.

**Figure 7.8-2 Automatic D3 Mitigation Block Diagram<sup>4</sup>**



<sup>4</sup> Generated from D3-Topical Report Figure 2-1, Figure 4-1, and Figure 4-2.

#### 7.8.4.1.2 *Diverse Displays and Manual Controls*

SRM Position 4, to SECY-93-087 states that a set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. These credited displays and controls shall be independent and diverse from the safety-related computer system. The guidance of SRP BTP-7-19 states that displays and manual controls provided for D3 conformance with SRM Item 18, Position 4 of SECY 93-087 should be sufficient both for monitoring the plant state and to enable control room operators to actuate the systems that will place the plant in a hot shutdown condition. In addition, the displays and controls should be sufficient for the operator to monitor and control the following critical safety functions:

- Reactivity control / level
- Core heat removal
- Reactor coolant inventory
- Containment isolation
- Containment integrity

FSAR Tier 1, Section 2.4.2, "Safety Information and Control System," Interim Revision 3 mark-ups, states that the SICS is provided as a safety-related display and control system and is specifically designed to provide the operator with the necessary inventory of controls and indications for mitigation of postulated accidents concurrent with a SCCF of the PS in the MCR. FSAR Tier 2, Section 7.8.1.2.4, Interim 3 mark-ups, list Type A, B, and C post-accident monitoring variables as indications that are processed by the SCDS and sent to the SICS for display to the operator.

FSAR Tier 2, Section 7.5.2.2.1, Interim Revision 3 mark-ups, and Technical Report ANP-10304, Section 3.2.1.3 state that the guidance of RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Revision 4, June 2006, will be used to confirm the PAM variables during detailed system design. RG 1.97 endorses IEEE Std 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," as an acceptable method for providing instrumentation to monitor variables for accident conditions. IEEE Std 497-2002, Clause 4.2, "Type B Variables," states that Type B variables are those variables that provide primary information to the control room operators to assess the plant critical safety functions and that any plant critical safety functions addressed in the emergency procedure guidelines or the plant specific emergency operating procedures that are in addition to those identified for Type A variables shall also be included. In addition, FSAR Tier 2, Sections 7.8.1.1.3 and 7.8.1.2.4, Interim Revision 3 mark-ups, list the following indications as indications that are generated by the DAS and sent to the SICS for display to the operator:

- DAS status of automatically initiating RT and ESF functions
- DAS operation status (i.e., bypass, initiate, standby, normal)
- DAS power availability
- DAS system faults or messages pertinent to plant operation



- Alarms and indications that are processed by the DAS

Technical Report ANP-10304, Section 3.2.1.1 states that the controls on SICS to initiate a reactor trip are provided to address BTP 7-19, Point 4 . These controls consist of four switches that are each assigned to a division of the DAS. Technical Report ANP-10304, Section 3.2.1.2 states that manual system-level initiation of critical safety functions is available on the SICS are required to be diverse from the PS. FSAR Tier 2, Section 7.8, Interim Revision 3 mark-ups, describes how the DAS processes manual functions initiated from SICS. The operator initiates reactor trips, ESF actuations, component, and/or system-level critical safety function manual actuations from the SICS. Upon manual initiation from the SICS these signals are sent directly to the DAS, via a hardwired path, and the DAS performs the system-level actuation of the applicable safety functions. The non-safety-related portions of the SICS also provides component-level manual actuation control as well. This diverse manual signal path originates from the non-safety-related portion of the SICS and is sent directly to the corresponding component's PACS module via a hardwired connection that bypasses the PS digital processing components. Therefore, the DAS processes the manual system-level safety initiations generated from the SICS, and the PACS processes the component-level manual initiations generated from the SICS. Table 7.8-6 below lists the D3 manual actuations that are available to the operator in the MCR for D3 mitigation.

**Table 7.8-6 Credited D3 Manual Controls Available in the Main Control Room<sup>5</sup>**

<b>Plant Function Manually Initiated</b>	<b>Manually Initiated from System</b>	<b>I&amp;C System that Processes MCR Initiation</b>	<b>System-Level or Component</b>	<b>Critical Safety Function</b>
<b>Manual System-Level Actuation</b>				
Reactor Trip	SICS	DAS	System-Level	Reactivity Control
EFW	SICS	DAS	System-Level	Core Heat Removal
Medium Head Safety Injection	SICS	DAS	System Level	Reactor Coolant Inventory
Stage 1 Containment Isolation	SICS	DAS	System-Level	Containment Isolation
Opening Of Containment H2 Mixing Dampers	SICS	DAS	System-Level	Containment Integrity

<sup>5</sup> FSAR Tier 1, ITAAC Design Commitment Item 3.4, Interim Revision 3 mark-ups; FSAR Tier 2, Sections 7.8.1.1.1 and 7.8.1.2.3, Interim Revision 3 mark-ups, and Technical Report ANP-10304, Revision 4, Section A.2.2.

Plant Function Manually Initiated	Manually Initiated from System	I&C System that Processes MCR Initiation	System-Level or Component	Critical Safety Function
Manual Component Level Actuation				
Emergency Diesel Generator (EDG) Start	SICS	PACS	Component	
Component Controls to Support Diesel Generator Loading (Both EDG And Station Blackout)	SICS	PACS	Component	
EFW controls for Long-Term SG Level Control	SICS	PACS	Component	
Safety-Injection Switchover to Hot Leg Injection	SICS	PACS	Component	
Main Steam Isolation Valve (MSIV) Closure	SICS	PACS	Component	
Feedwater Isolation (Main Feedwater and EFW)	SICS	PACS	Component	
Control Of MHSI	SICS	PACS	Component	
Extend Partial Cooldown Controls	SICS	PACS	Component	
Depressurize RCS With Pressurizer Sprays	SICS	PACS	Component	
Actuation of Extra Borating System (EBS)	SICS	PACS	Component	
Control Room HVAC	SICS	PACS	Component	

Plant Function Manually Initiated	Manually Initiated from System	I&C System that Processes MCR Initiation	System-Level or Component	Critical Safety Function
Reconfiguration				
Chemical Volume Control System Isolation	SICS	PACS	Component	
Main Steam Relief Trains Controls	SICS	PACS	Component	

Technical Report ANP-10304, Section 4.1 states that all manual control functions credited in the D3 analysis are performed from the SICS. Accordingly, based on the design commitment to implement MCR indications according to the guidance of RG 1.97, the commitment to display DAS status and plant process indications in the MCR, and the inventory of manual control system actuations to control plant critical safety functions from the MCR, the staff finds that the applicant's D3 control and display design addresses the BTP 7-19 guidance for available displays and controls.

#### 7.8.4.1.2.1 SICS Manual Controls and Display

SICS contains both safety-related and non-safety-related equipment, and it is a human-machine interface located in the MCR and the RSS. FSAR Tier 2, Section 7.1.1.3.1 states that SICS is implemented with the TXS digital I&C platform and hardwired I&C equipment. The TXS platform is the platform that is used to implement PS. Technical Report ANP-10304, Figure 2-1 provides a single line diagram of the SICS manual control and indication display signal paths.

SICS is a HMI located in the MCR for operator indications and plant system and component controls. The SICS only displays sensor and plant process measurements and operating status and does not perform setpoint calculations, does not perform a "vote" count for system or component actuation, nor is it designed to self-initiate plant safety functions. SICS is not designed to automatically actuate plant safety functions. Therefore, SICS is fundamentally different in purpose than the PS. Due to SICS being fundamentally different in purpose than the PS, this would inherently warrant a different design approach than the PS. Accordingly, the staff finds that there is sufficient diversity between PS and SICS with respect to different approaches within the same technology and different architecture. In addition, staff also finds sufficient diversity between the systems as it relates to different purpose, function, control logic, or actuation means and same manufacturer of fundamentally different designs.

Technical Report ANP-10304, Revision 4, Table 2-1 states that the SICS digital indicators will have TXS technology that can include programmable electronic I&C technology, which, according to FSAR Tier 2, Section 7.1, Interim Revision 3 mark-ups, can be TXS microprocessor-based. However, Technical Report ANP-10304, Section 4.2 states that the indications provided in SICS are performed by hardwired, analog components. Therefore, in RAI 505, Question 07.08-43, the staff requested that the applicant clarify this discrepancy. The staff also requested that the applicant clarify the TXS technology that can be used in SICS. To address these issues, **RAI 505, Question 07.08-43 is being tracked as an open item.** In

addition, the staff's review could not locate design descriptions demonstrating how the SICS equipment will be implemented with different TXS logic processing equipment than the PS. Therefore, staff does not find sufficient diversity associated with logic processing equipment diversity between the SICS and PS.

Technical Report ANP-10304, Revision 4, Section 4.2 credits the use of different engineers for human diversity between the SICS and the PS. Accordingly, the staff finds sufficient diversity between the SICS and PS related to different design and development teams.

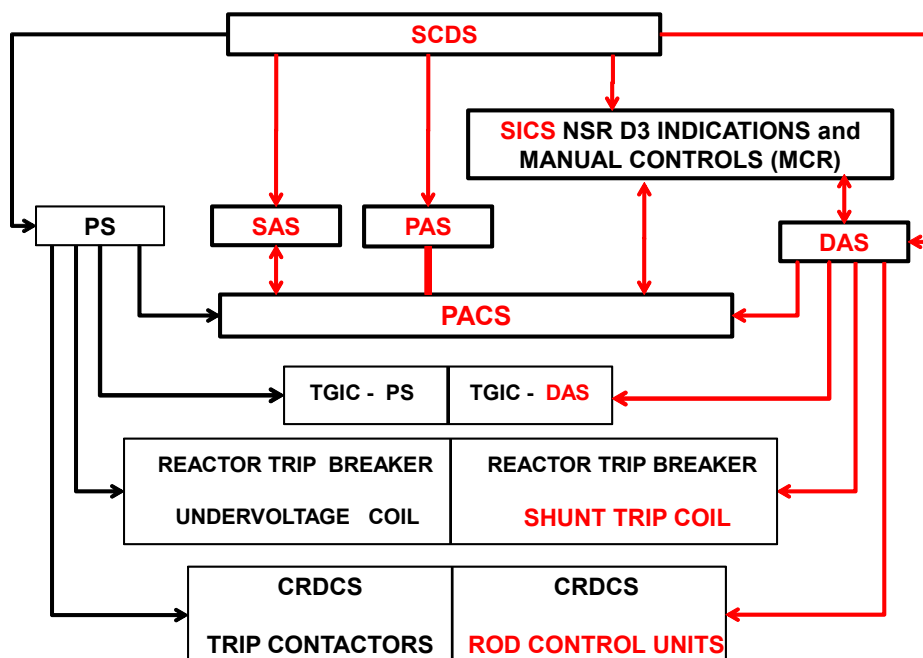
Technical Report ANP-10304, Section 4.2 states that the SICS uses hardwired, analog I&C components, and, with the exception of the qualified display system (not credited in the D3 assessment), there is no software running in the SICS. In addition, Technical Report ANP-10304, Figure 2-1 shows that SICS credited D3 indications are hardwired directly from the SCDS and do not originate from or pass through the PS. Therefore, based on the different purpose, functionality, absence of operational software in the SICS, and signal paths that are not associated with PS processing equipment, the staff finds that the SICS platform implementation is adequately diverse from the PS.

The guidance of BTP 7-19 states that the point at which the manual controls are connected to safety-related equipment should be downstream of the plant's digital I&C safety-related system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. To achieve system-level actuation at the lowest possible level in the safety-related system architecture, the controls may be connected either to discrete hardwired components or to simple (e.g., component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.

FSAR Tier 2, Section 7.1.1.3.1, Interim Revision 3 mark-ups, states that SICS manual controls are implemented with buttons and switches and the controls required to be on the SICS are implemented with dedicated, hardwired I&C. Technical Report ANP-10304, Table 2-1 states that SICS manual controls are implemented with electrical technology, which, according to FSAR Tier 2, Section 7.1, Interim Revision 3 mark-ups, is based on electro-mechanical components. Technical Report ANP-10304, Sections 3.2.1.1 and 3.2.1.2 state that DAS reactor trip controls on the SICS are assigned to DAS divisions and DAS ESF controls on the SICS are combined with the automatic actuation logic in DAS. Technical Report ANP-10304, Figure 2-1 "U.S. EPR DCS Functional Architecture," indicates that the DAS credited SICS controls are located on the non-safety related portion of the SICS. Therefore, the credited, manual diverse signal path from the SICS to the DAS is a hardwired path that originates from the non-safety related portion of the SICS, bypasses the PS software-based processing equipment, and is hardwired directly to the DAS. Technical Report ANP-10304, Figure 2-1 also shows that the DAS manual controls located on the SICS for manual component controls are hardwired directly to the PACS. FSAR Tier 2, Section 7.1.1.3.1, Interim Revision 3 mark-ups, states that the non-safety-related portion of the SICS is powered from the 12-hour uninterruptible power supply of which the staff's review finds that this non-safety-related power supply is independent of the SICS safety-related power supply. Therefore, based on the diverse D3 manual control signal paths that are not affected by a PS SCCF, and the independent power supply for the non-safety related SICS DAS controls, the staff finds that the SICS diverse manual control implementation addresses the BTP 7-19 guidance for diverse controls being downstream of the plant's digital I&C safety-related system outputs and their connections do not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment.

Based on the staff's findings listed in this section for sufficiency of D3 diverse plant parameter displays and indications in the MCR, the sufficiency of displays and controls in the MCR to monitor and control system-level actuation of critical safety functions, and the adequacy of the diversity and independence of these D3 credited indications and controls, the staff finds that the credited SICS D3 diverse design adequately addresses SRM Item II.Q, Position 4, to SECY-93-087. In addition, based on staff's finding for adequate and sufficient SICS displays and controls with direct system-to-system hardwired connections, the staff finds that failure of monitoring or display systems will not influence the functioning of the primary reactor trip systems or the ESF actuation systems. The staff's findings for diverse D3 mitigation I&C system is illustrated in Figure 7.8-3 below, which is based on Technical Report ANP-10304, Figures 2-1, 4-1, and 4-2.

**Figure 7.8-4 D3 Mitigation Systems <sup>6</sup>**



#### 7.8.4.2 D3 Best Estimate Analysis

10 CFR 50.62 requires, in part, diverse equipment to automatically respond to ATWS events. GDC 22 requires in part that the effects of postulated accident conditions on redundant channels do not result in loss of the protection function and that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function. IEEE Std 603-1998, Clause 5.16 requires, in part, that plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure. Item II.Q, Position 2 of the SRM to SECY-93-087 states:

In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident

<sup>6</sup>Generated from Technical Report ANP-10304, Figure 2-1, Figure 4-1, and Figure 4-2; and FSAR Tier 2, Figure 7.1-11, Interim Revision 3 mark-ups.

analysis section of the safety analysis report (SAR) using best estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

The staff evaluated the ability of the applicant's credited I&C D3 mitigation systems to mitigate AOOs and PAs, concurrent with a SCCF of the PS. To address the D3 mitigation plant response to a CCF of the PS, staff used the guidance found in SRP BTP 7-19, Section B.3, Items 1 and 2. The staff also used the guidance in NUREG/CR-6303 to evaluate the adequacy and sufficiency of credited I&C system diversity to address the acceptance criteria of SRP BTP 7-19. NUREG/CR-6303, Guidelines 5 and 6 describe the method for postulating CCF of the I&C system using the block diagram of the protective system.

Technical Report ANP-10304, Section 4.11.1 states that the applicant only considers SCCFs that can credibly be assumed to occur in the PS concurrent with an AOO or PA in the D3 plant response analysis. The applicant's D3 plant response analysis does not consider environmental triggers that could cause a SCCF. The applicant states that for a CCF to occur, two conditions must be present: (1) An identical, latent defect must exist in multiple redundancies of a system and (2) a triggering condition must occur, in multiple redundancies, which exposes the latent defect. The applicant concludes that if one of the two conditions does not exist, a failure does not occur.

Technical Report ANP-10304, Section A.2.1 states that best-estimate models and methods are utilized, including:

- initial nominal full power operating condition (without uncertainty)
- no preventive maintenance being performed on plant equipment
- no occurrence of a single failure
- nominal reactor trip setpoints
- control rods fully withdrawn except for partial insertion of lead bank
- best estimate neutronics parameters and power distributions
- no hot channel factors for engineering uncertainty or rod bow
- equilibrium cycle core conditions

The staff requested the applicant to provide addition details and descriptions of how the best-estimate initial condition assumptions used in the D3 analyses were generated in RAI 413, Question 07.08-19. The March 23, 2011, proprietary response to RAI 413, Question 07.08-19 provided a detailed description of the following best-estimate initial condition assumptions used in the D3 analyses:

- Core average axial and core radial power distributions and reactivity coefficient curves
- The core average axial power distributions
- The reactivity coefficient curves (MTC, Doppler)

- The hot channel factors,  $F\Delta h$  and  $FQ$
- The scram reactivity curves and the total scram reactivity worth ( $\Delta\rho$  or pcm)
- The non-fuel-related reactor core parameters affecting DNBR, including  $T_{inlet}$ , reactor system pressure, and total core flow
- An assessment of the initial steady-state DNBR operating margin with the best-estimate assumptions and comparison to the expected Technical Specification (TS 3.2.3) DNBR limiting condition for operation value

SRP BTP 7-19 allows for the use of best-estimate methods, and does not stipulate a need for uncertainty analysis. With the exception of the use of nominal reactor trip setpoints, the staff finds the above-listed assumptions acceptable for use in this methodology. The D3 plant response is analyzed until a stable controlled condition is achieved. Technical Report ANP-10304, Section A.2.1 defines a stable controlled condition as:

- Reactor is subcritical and remains subcritical.
- Core is covered.
- Decay heat is being removed from the RCS.
- Secondary inventory levels are sufficient to maintain RCS temperatures.
- During large break LOCA, SI is maintaining core temperatures.

There are several cases that reach a new steady-state condition without a reactor trip. These are also considered stable controlled conditions. For loss-of-coolant accidents, the end-state corresponds to a depressurized RCS with safety injection providing make-up for maintaining RCS inventory and core cooling. For a SG tube rupture, after initial stabilization, the plant is required to cool down and establish residual heat removal cooling. In addition to providing a description of the initial condition assumptions, a comparison of each of the above parameters to their respective design values as contained in the FSAR was provided. The staff reviewed the information and concluded that all of the initial condition assumptions being used by the applicant were reasonable and acceptable for the D3 analysis. SRP Section 7.8 guidance states that the applicant should identify the D3 plant response:

- Bounding and bases events that are presented or referenced in SAR Chapter 15.
- The range of transient and steady-state conditions for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform.

The staff's review found that the applicant's stated bounding events and bases, as listed above, address the guidance of SRP Section 7.8.

Technical Report ANP-10304, Section A.2.2 lists the credited D3 DAS automatic functions, which are also provided below:

- Reactor trip on low SG pressure

- Reactor trip on low SG level
- Reactor trip on high SG level
- Reactor trip on low RCS flow (two loops)
- Reactor trip on low-low RCS low (one loop)
- Reactor trip on high neutron flux (power range)
- Reactor trip on low hot leg pressure
- Reactor trip on high pressurizer pressure
- Turbine trip on reactor trip
- EFW system actuation on low SG level
- Safety injection system actuation on low pressurizer pressure
- Main steam isolation on low SG pressure
- Containment isolation on high activity
- Main feedwater isolation on low SG pressure (affected generator)
- Main feedwater isolation on high SG level (affected generator)
- Opening of containment hydrogen mixing dampers on high containment pressure
- Opening of containment hydrogen mixing dampers on differential pressure
- Start station blackout diesel generators

PAS and SAS automatic D3 control functions are described in Technical Report ANP-10304, Table A.2.2. Technical Report ANP-10304, Table A.2-3 includes the DAS setpoint values used in the D3 plant response transient analysis. The AOOs and PAs analyzed in the presence of a SCCF of the PS are those evaluated in FSAR Tier 2, Chapter 15. Technical Report ANP-10304, Section A.2.5 states that the computer codes used for the D3 analysis are the same as those used in FSAR Tier 2, Revision 2, Chapter 15, safety analysis. However, the applicant stated that minor changes were made to the S-RELAP5 code to reflect improved heat transfer in the SG secondary system. In RAI 413, Question 07.08-21, the staff requested that the applicant provide a description of these changes. In a March 23, 2011, response to RAI 413, Question 07.08-21, the applicant provided proprietary design descriptions and justifications of the modifications made to the S-RELAP5 code requested by the staff, and the staff finds that the applicant's March 23, 2011, response RAI 413, Question 07.08-21, acceptable and the altered S-RELAP5 computer codes used in the D3 assessment acceptable. Technical Report ANP-10304, Table A.2-1, "U.S. EPR Initiating Events," lists the category, event, and section located, for each D3 event analyzed within Appendix A of the same report. The criterion for meeting primary coolant system integrity is 120 percent of design (17.58 MPa, (2,535 psig)), which is slightly under the ASME Service Level C limit of 22.16 MPa (3,200 psig) and consistent with the acceptance criterion for ATWS, as specified in SRP Section 15.8. The



criterion for meeting containment structure integrity is the ultimate pressure capacity, consistent with SRP Section 3.8.1. The ultimate pressure capacity is cited in Technical Report ANP-10304, Section A.2.4, is 1.18 MPa (156 psig), or 2.52 times the containment design pressure. The design pressure of 0.53 MPa (62 psig) is consistent with the value given in FSAR Tier 2, Section 3.8.1.1. The applicant also identifies a secondary system peak pressure acceptance criterion of 120 percent of the secondary system design pressure (consistent with ASME Service Level C), which is 10 MPa (1450 psia).

Technical Report ANP-10304, Section A.3 provides the D3 plant response analysis results for each of the following categories; similarly provided for the design basis events in FSAR Tier 2, Revision 2, Chapter 15:

- Increase in Heat Removal by Secondary System
- Decrease in Heat Removal by Secondary System
- Decrease in RCS (RCS) Flow Rate
- Reactivity and Power Distribution Anomalies
- Increase in RCS Inventory
- Decrease in RCS Inventory
- Radiological Consequences

An evaluation of the events by category is provided in the paragraphs below.

#### *7.8.4.2.1 Increase in Heat Removal by Secondary System*

The DBEs evaluated in this category of events are:

- decrease in Feedwater (FW) Temperature
- increase in FW Flow
- increase in Steam Flow
- inadvertent SG MSRV Opening (including inadvertent MSRT actuation)
- steam System Piping Failure

All these events are classified as AOOs with the exception of the Steam System Piping Failure, which is a PA.

In Technical Report ANP-10304, Section A.3.2.1, the applicant provides an engineering argument that the "Decrease in FW Temperature" event results in a less limiting DNBR transient than the "Increase in Steam Flow" event. With a SCCF assumed for the D3 analysis, the event proceeds in the absence of Low-DNBR reactor trip. Core power level will continue to increase to a maximum level corresponding to the DAS High Neutron Flux reactor trip. Considering the rate of the transient and the effects on thermal margin, the staff concurs that the increase in steam flow event poses a more severe challenge to fuel thermal parameters.

For the “Increase in FW Flow” event (Technical Report ANP-10304, Section A.3.2.2), DAS provides a backup reactor trip that terminates the transient, although somewhat later than as presented in FSAR Tier 2, Chapter 15 design basis event analysis. The added margin to the Specified Acceptable Fuel Design Limits (SAFDLs) associated with D3 best-estimate assumptions; coupled with the backup DAS reactor trip, ensure that the applicable acceptance criteria are met.

For the “Increase in Steam Flow” event (Technical Report ANP-10304, Section A.3.2.3), the applicant provides an explicit D3 engineering analysis. In comparison to FSAR Tier 2, Chapter 15 analysis, the D3 analysis with SCCF does not result in a reactor trip. The Low DNBR, High SG Pressure Drop, and High Core Power Level trips that would actuate through the PS are assumed to be unavailable, and the DAS high neutron flux trip does not respond due to decalibration of the ex-core neutron detectors resulting from the lower vessel downcomer temperatures. The D3 analysis results show that the reactor reaches a steady state operating condition at approximately 130 percent power, which the operator is eventually expected to terminate via manual trip actuation. The staff finds this action reasonable, given the availability of the displays and controls in the main control room, as discussed in Section 7.8.4.1.2 of this report. The applicant’s March 23, 2011, response to RAI 413, Question 07.08-38 addressed the staff’s request for a description of how the decalibration of the ex-core neutron detectors is incorporated into the “Increase in Steam Flow” analysis. The staff also noted that neither beginning of cycle (BOC) nor end of cycle (EOC) conditions are necessarily the conditions that are most challenging to the specified acceptable fuel design limits SAFDLs. Rather, the limiting condition is one which leads to a stabilization of the indicated neutron flux signal just below the reactor trip setpoint. The applicant provided a simulation of this condition in the March 23, 2011, response to RAI 413, Question 07.08-38, and added it to Technical Report ANP-10304. The staff finds that the applicant’s March 23, 2011, response to RAI 413, Question 07.08-38 addresses its concerns, and is therefore acceptable. The staff considers RAI 413, Question 07.08-38 resolved.

Technical Report ANP-10304 states that no fuel failure is predicted for the “Increase in Steam Flow” event. In comparing the core power levels and the DNBR transients for both the Chapter 15 safety analysis and the D3 analysis, the staff was unable to confirm that the DNBR SAFDL would not be exceeded. Therefore, in RAI 413, Question 07.08-22, the staff requested that the applicant provide additional information in order to complete the staff’s review of the “Increase in Steam Flow” event. In a March 23, 2011 response RAI 413, Question 07.08-22, the applicant provided plots of the normalized minimum DNBR and maximum LPD to the corresponding SAFDL for the “Increase in Steam Flow” D3 analysis, thereby demonstrating that SAFDLs were not violated. The response noted that the margin in the DNBR and the LPD for the increased steam flow event in the D3 analysis and FSAR Tier 2, Chapter 15 safety analysis are due to the usage of best-estimate versus bounding power distributions and to how uncertainties are applied in the two analyses. The applicant’s response clearly demonstrated that SAFDLs were not violated in the D3 increase in steam flow analysis. Therefore, the staff finds the applicant’s March 23, 2011, response to RAI 413, Question 07.08-22 acceptable. The staff considers RAI 413, Question 07.08-22 resolved.

The “Inadvertent SG MSRV (Main Safety Relief Valve) Opening” event is addressed in Technical Report ANP-10304 Section A.3.2.4 through an engineering argument stating that the event is bounded by the “Increase in Steam Flow” event (addressed above) prior to the point of reactor trip and by the “Steam System Piping Failure” during its potential return-to-power following reactor trip. The “Increase in Steam Flow” event is analyzed assuming full opening of

all turbine bypass valves with a total capacity of 60 percent of full steam load, which is greater than the capacities of either an MSRT or an MSRV.

In Technical Report ANP-10304, Section A.3.2.5, an engineering argument is presented to address the “Steam System Piping Failure” event, or main steam line break (MSLB). The MSLB is evaluated assuming full power reactor operation with D3 best-estimate conditions. Two key differences between Technical Report ANP-10304 and FSAR Tier 2, Chapter 15 safety analyses, are as follows:

- MSLB at Hot Zero Power (HZIP) is not evaluated in the D3 analysis
- All control rods fully insert upon reactor trip (no stuck rod) in the D3 analysis

The absence of a stuck rod significantly reduces the severity of the MSLB event because greater shutdown margin is available to prevent both a return to criticality and the extreme power peaking that would result in the vicinity of a stuck rod. Considering the use of best-estimate conditions, including HFP conditions the applicant’s analysis concluded that no fuel failures are expected to occur. In RAI 413, Question 07.08-23, the staff requested, in part, that the applicant provide information regarding the MSLB case with PS SCCF at full power conditions to demonstrate that a return to criticality does not occur following reactor trip. In a February 1, 2011, response to RAI 413, Question 07.08-23, the applicant provided the details of the analysis of the MSLB event, providing a table of core reactivity as a function of core moderator temperature. The table demonstrates that the core remains in a negative reactivity state until its temperature falls below 40.6°C (105 °F). Since this temperature is well below the saturation temperature at atmospheric pressure, it is not possible for the SGs to cool the primary system to this temperature. Therefore, re-criticality cannot occur during an MSLB under best-estimate assumptions.

In summary, for the “Increase in Heat Removal by Secondary System” category of events, the staff finds:

- that the BTP 7-19 best-estimate plant response analysis acceptance criteria are met
- no operator actions are required as a diverse means of protective action<sup>7</sup>

#### *7.8.4.2.2 Decrease in Heat Removal by Secondary System*

The DBEs evaluated in this category of events are:

- loss of External Load/Turbine Trip
- loss of Condenser Vacuum
- closure of Main Steam Isolation Valve
- loss of Non-Emergency AC Power

---

<sup>7</sup> Operator action as a diverse means of protective action means an operator action which is required to perform a safety function normally performed by the PS in order to meet acceptance criteria. Operator actions to bring the plant to safe shutdown are not necessarily diverse means of protective action.

- loss of Normal FW Flow
- FW System Pipe Break

All these events are classified as an AOO with the exception of the FW System Pipe Break, which is a PA.

Technical Report ANP-10304, Section A.3.3.1 provides an engineering argument to address the Loss of External Load, Turbine Trip, and Loss of Condenser Vacuum events. FSAR Tier 2, Chapter 15 safety analyses of these three events shows that the Turbine Trip is most limiting, with a PS reactor trip actuation on High Pressurizer Pressure. Since DAS also provides a High Pressurizer Pressure trip (40 psi higher than the PS value), adequate protection is provided. The D3 analysis also assumes operation of the turbine bypass system, which would further mitigate the limiting Turbine Trip event. With the condenser not available for the Loss of Condenser Vacuum event, the transient is similar to FSAR Tier 2, Chapter 15 case. The increase in RCS and secondary side pressure remain well within acceptance criteria and the DNBR SAFDL is not challenged by the Loss of External Load, Turbine Trip, and Loss of Condenser Vacuum events with concurrent PS SCCF.

The Inadvertent Closure of an MSIV event analyzed in FSAR Tier 2, Chapter 15 safety analysis results in PS reactor trip actuation (at approximately 6 seconds) on High SG Pressure, which is not available through DAS. Therefore, an explicit D3 analysis is provided in Technical Report ANP-10304, Section A.3.3.2 for the Inadvertent Closure of an MSIV event. The D3 analysis shows that at approximately 130 seconds DAS provides a reactor trip actuation on Low SG Level. The pressure in the affected SG reaches approximately 11.31 MPa (1,640 psia), or 113 percent of the secondary system design pressure (design pressure is 10.0 MPa (1,450 psia), per FSAR Tier 2, Table 10.3-1). Considering the high rate of change of the SG pressure excursion and its calculated peak value relative to the D3 analysis criterion (11.31 MPa (1,640 psia) calculated peak SG pressure versus the 12.0 MPa (1,740 psia) criterion), in RAI 413, Question 07.08.-24, the staff requested that the applicant provide additional information on the SG level model and the DAS Low SG Level trip function in order to complete the staff's review of the "Inadvertent Closure of an MSIV" D3 analysis. In a January 28, 2011, response to RAI 413, Question 07.08-24, the applicant provided a description of the two level models used to compute the SG level. One model mimics the actual plant instrumentation in that it uses differential pressure to compute SG level. The other model uses the collapsed level in the SG downcomer. The staff reviewed both models and concluded that each provided a reasonable simulation of the SG level response during plant transients. In particular, the staff finds that the applicant's simulation of the SG level and the low level trip for the "Inadvertent Closure of an MSIV" event is reasonable. Therefore, the staff finds RAI 413, Question 07.08-24 acceptable and considers the issue resolved.

The Loss of Non-Emergency AC Power to Station Auxiliaries event is addressed in Technical Report ANP-10304, Section A.3.3.3. The loss of power to the non-emergency buses results in an immediate coastdown of the reactor coolant pumps and termination of main feedwater to the SGs. In FSAR Tier 2, Chapter 15 safety analysis, a prompt reactor trip actuation on Low RCP Speed and automatic startup of the emergency diesel generators occurs. As described in FSAR Tier 2, Section 7.3.1.2.12, the PS monitors voltage levels on the four divisional Class 1E Emergency Power Supply System buses (normally fed by offsite power) and issues a LOOP signal directly to the emergency diesel generators upon voltage degradation. For the D3 analysis with a SCCF, DAS initiates a reactor trip on Low RCS Flow a few seconds after loss of the reactor coolant pumps. However, because the automatic emergency diesel generator

startup is initiated through a LOOP signal provided by the PS, the emergency diesel generators must be started manually and the EFW pumps loaded to the buses manually. FSAR Tier 2, Sections 7.3.1.2.12 and 7.8.1.2.3, Interim Revision 3 mark-ups, state that the emergency diesel generators are manually started through SICS in the MCR. Technical Report ANP-10304, Section A.3.3.3 also states that the two station blackout diesel generators start automatically upon loss of AC power, but the EFW pumps need to be manually loaded to the station blackout diesel generators. According to FSAR Tier 2, Section 8.4.1.1, and as stated in Technical Report ANP-10304, Section A.3.3.3, only two of the four EFW pumps may be loaded onto the station blackout diesel generator buses. The applicant reports that it would take at least 1½ hours for the SGs to boil dry for loss of reactor system heat sink, providing sufficient time to manually initiate EFW. In RAI 413, Question 07.08-25, the staff requested that the applicant identify the credited diverse means to address LOOP, consistent with this information. In a February 1, 2011, response to RAI 413, Question 07.08-25, the applicant noted that emergency procedure guidelines/emergency operating procedures are still under development for the U.S. EPR, so a definitive operator response time to start the emergency diesel generators is not available. However, it is reasonable to expect this time to be well within the 1½ hours it takes for the SGs to boil dry. Even if the SGs were to boil dry, the operator could resort to feed-and-bleed operation to control primary system pressure. The staff concurs with the applicant's assessment that there is ample time for manual operator action prior to SG dryout.

Technical Report ANP-10304, Section A.3.3.4 provides an engineering argument for the "Loss of Normal FW Flow" event. Like the analysis presented in FSAR Tier 2, Section 15.2.7, the "Loss of Normal FW Flow" event results in a reactor trip actuation on Low SG Level. Fuel SAFDLs (DNBR and LPD) are not challenged because there is no increase in reactor power. DAS provides the Low SG Level trip function and automatic start of EFW. Secondary system pressure is controlled by the turbine bypass system in the D3 analysis. As in FSAR Tier 2, Chapter 15 safety analysis, operator control of EFW system is eventually required. Given the best-estimate assumptions, the D3 analysis of the "Loss of Normal FW Flow" event is bounded by the FSAR results.

The "FW System Piping Failure" is classified as a PA. FSAR Tier 2, Section 15.2.8 provides an analysis of a spectrum of feedwater system piping size failures. In all cases, except the limiting SG overpressure case, DAS provides an equivalent reactor trip function and EFW actuation to mitigate the event. For the limiting SG overpressure case, FSAR Tier 2, Chapter 15 analysis shows a reactor trip on SG pressure drop, which is not provided in DAS. Considering the availability of the DAS Low SG Pressure reactor trip function and the application of best-estimate analysis assumptions, the D3 analysis can reasonably be expected to be bounded by FSAR Tier 2, Chapter 15 safety analysis of the Feedwater System Piping Failure analysis. Operator actions to control EFW are similar to that assumed in the FSAR analysis.

In summary, for the Decrease in Heat Removal by Secondary System category of events, the staff finds:

- that the BTP-7-19 best-estimate plant response acceptance criteria are met
- no operator actions are required as a diverse means of protective action

#### *7.8.4.2.3 Decrease in RCS Flow Rate*

The DBEs evaluated in this category of events are:

- partial Loss of Forced RCS Coolant Flow

- complete Loss of Forced RCS Coolant Flow
- RCP Rotor Seizure or RCP Shaft Break

The loss of forced RCS flow events are classified as AOOs while the pump seizure or shaft break events are classified as PAs. In all of the events, the sudden drop in reactor core flow results in a challenge to the DNBR SAFDL.

FSAR Tier 2, Section 15.3.1 analysis of the loss of a single RCP shows that a PS reactor trip actuation occurs on Low-Low RCS Flow (one loop). While DAS provides the same Low-Low RCS Flow trip function, its setpoint is slightly lower than the PS trip, but the use of best-estimate assumptions in the D3 analysis tend to offset the later DAS trip actuation.

Technical Report ANP-10304, Section A.3.4.2 provides an analysis of the “Complete Loss of Forced RCS Flow” event, and states that no fuel failures occur. The staff determined that the applicant’s analysis provided insufficient information on the DNBR transient for the staff to complete its evaluation of the Complete Loss of Forced RCS Flow event. Therefore, in RAI 413, Question 07.08-26, the staff requested that the applicant provide additional information to clarify this issue. In a March 23, 2011, response to RAI 413, Question 07.08-26, the applicant provided a comparison to FSAR Tier 2, Chapter 15 safety analysis, and the D3 analyses of the event, along with a plot of the minimum DNBR for the D3 analysis. The improvement of the DNBR response in the D3 analysis relative to FSAR Tier 2, Chapter 15 analysis, was demonstrated to be due to best-estimate assumptions for RCS flow, bypass flow, scram reactivity, moderator reactivity coefficient, and core power distribution. The staff reviewed the March 23, 2011, response to RAI 413, Question 07.08-26, and finds the applicant’s analysis and conclusions regarding the complete loss of flow event complete and reasonable. Therefore, the staff finds the response acceptable, and considers RAI 413, Question 07.08-26 resolved.

The “RCP Rotor Seizure” event, which is more limiting than an “RCP Shaft Break”, is mitigated by either a PS or DAS actuated Low-Low RCS Flow (one loop) reactor trip. Although the DAS reactor trip occurs slightly later for the D3 analysis, the best-estimate assumptions tend to offset the effects of the later trip. FSAR Tier 2, Section 15.3.3, analysis shows that the sudden drop in core coolant flow results in the DNBR SAFDL being exceeded with approximately eight percent of the fuel rods conservatively estimated to fail. In RAI 413, Question 07.08-27, the staff requested that the applicant provide additional information in order to complete the staff evaluation of the “RCP Rotor Seizure D3” event. In a March 23, 2011, response to RAI 413, Question 07.08-27, the applicant provided a comparison of the assumptions in the Technical Report ANP-10304 analysis and FSAR Tier 2, Chapter 15 safety analysis, and showed which best-estimate assumptions were responsible for the higher minimum DNBR in the D3 analysis. Based upon its review of the March 23, 2011, response to RAI 413, Question 07.08-27, the staff concludes that the best-estimate plant response acceptance criteria for BTP 7-19 are met for the “RCP Rotor Seizure” event. Therefore, the staff considers the applicant’s March 23, 2011, response to RAI 413, Question 07.08-27 acceptable and considers the issue resolved. In summary, for the Decrease in RCS Flow Rate category of events, the staff finds:

- that the BTP-7-19 best-estimate plant response acceptance criteria are met
- no operator actions are required as a diverse means of protective action

#### 7.8.4.2.4 *Reactivity and Power Distribution Anomalies*

The DBEs evaluated in this category of events are:

- Uncontrolled RCCA Withdrawal from Subcritical or Low-Power Startup Condition
- Uncontrolled RCCA Withdrawal at Power
- RCCA Misoperation
- Startup of an Inactive RCP at an Incorrect Temperature
- CVCS Malfunction Resulting in Decreased RCS Boron Concentration
- RCCA Ejection

All these events are classified as AOOs with the exception of the “Control Rod (RCCA) Ejection,” which is classified as a PA. An evaluation of the uncontrolled RCCA withdrawal from subcritical or low-power startup condition event is not provided because the best-estimate analysis in Technical Report ANP-10304 does not consider plant conditions below full power. The “Uncontrolled RCCA Withdrawal at Power” event is analyzed assuming full power initial conditions at both beginning-of-cycle and end-of-cycle conditions, and with the RCCAs inserted to the Technical Specification Power Dependent Insertion Limit (PDIL). The time in cycle affects moderator temperature coefficient and control rod bank worth. FSAR Tier 2, Section 15.4.2 analysis, states that the reactor system is protected by PS Low DNBR, High LPD, ex-core high rate of change, high core power level, and high pressurizer level reactor trip functions, none of which are provided by the DAS. Technical Report ANP-10304, Section A.3.5.2 engineering analysis shows that DAS actuates a reactor trip on Low SG Level and that reactor power peaks at approximately 108 percent. In RAI 413, Question 07.08-28, the staff requested that the applicant provide additional information in order to complete the staff review of uncontrolled RCCA withdrawal at power analysis. In a March 23, 2011, response to RAI 413, Question 07.08-28, the applicant provided a comparison of FSAR Tier 2, Chapter 15 safety analysis, and the Technical Report ANP-10304 analysis of the “Uncontrolled RCCA Withdrawal” event. The staff noted that the initial DNBR in the D3 analysis is 1.8 times the value in the safety analysis due to the best-estimate assumptions used in the D3 analysis. Another key difference in the analyses is that the D3 analysis limits the reactivity addition due to RCCA withdrawal to the worth of the length of the control rods withdrawn from the PDIL. FSAR Tier 2, Chapter 15 safety analysis, conservatively assumes reactivity addition continues until the reactor is tripped, even though the rods have been completely withdrawn earlier. The applicant’s March 23, 2011, response to RAI 413, Question 07.08-28 demonstrates how FSAR Tier 2, Chapter 15 safety analysis, bounds the D3 analysis of the uncontrolled RCCA withdrawal event. Therefore, the staff finds the applicant’s March 23, 2011, response to RAI 413, Question 07.08-28 acceptable and considers the issue resolved.

Technical Report ANP-10304, Section A.3.5.3 includes a D3 analysis of the “Dropped RCCA” event. In FSAR Tier 2, Chapter 15 analysis, the PS actuates a reactor trip on low DNBR, which is unavailable in the DAS. The limiting case, as reported in Technical Report ANP-10304, Section A.3.5.3, is the drop of a full bank of RCCAs from the PDIL position. The D3 analysis of this event shows that following the drop of the RCCA bank, the reactor power returns to full power with no reactor trip actuation. The applicant reports that the best estimate conditions offset the failure of the PS trip functions, and no fuel failures occur. In RAI 413, Question 07.08-29, the staff requested that the applicant provide additional information in order

to complete the staff review of the dropped RCCA D3 analysis presented in Technical Report ANP-10304, Section A.3.5.3. In a March 23, 2011, response to RAI 413, Question 07.08-29, the applicant provided a description of the RCSL response during the dropped RCCA event analysis, a comparison of initial and minimum DNBR for the analysis, and an explanation of why the drop of a RCCA bank was more limiting than the drop of a single RCCA. The response provided the information the staff needed to complete its review. Therefore the staff finds the response acceptable and considers RAI 413, Question 07.08-29 resolved.

FSAR Chapter 15 analysis of the startup of an inactive RCP at an incorrect temperature does not result in a reactor trip. Therefore, the failure of the PS does not affect the results of the event and a D3 analysis is not necessary.

Technical Report ANP-10304, Section A.3.5.5 provides a D3 engineering analysis of the boron dilution event. The D3 engineering analysis presented in Technical Report ANP-10304, Section A.3.5.5 indicates that the reactor transient (power level, coolant temperatures) is bounded by uncontrolled RCCA withdrawal event analyzed in Technical Report ANP-10304, Section A.3.5.2. No credit is taken in the D3 analysis for the response of the anti-dilution mitigation (ADM) system, as ADM relies on calculated boron concentrations provided by the PS. In addition to potentially challenging the DNBR SAFDL, the boron dilution transient can erode shutdown margin. Technical Report ANP-10304, Section A.3.5.5 suggests that with RCSL in operation, RCCAs will be automatically inserted and the operator will be alerted to the dilution event due to RCCA movement. In RAI 413, Question 07.08-30, the staff requested that the applicant clarify why the RCSL, which depends upon the PS for its actuation signal and is not credited as a diverse system, is assumed to be available. In a January 28, 2011, response to RAI 413, Question 07.08-30, the applicant identified that in the event of a SCCF that caused a complete failure of the PS, the RCSL would not operate. On the other hand, if the SCCF caused only partial failure of the PS, the RCSL might receive a signal to respond to an increase in core reactivity due to boron dilution. However, Technical Report ANP-10304, the applicant states that both the PS subsystems and the RCSL are not credited as diverse systems and are not credited to provide any D3 mitigation actuations. Therefore, the staff did not consider any mitigation actions from these systems in its evaluation or its findings and/or conclusions. Therefore, the staff finds that this event is bound by the "Uncontrolled RCCA Withdrawal" event. Technical Report ANP-10304, Section A.3.5.5 also describes the case where RCCA control is in manual (no credit for RCSL), and states that the continued dilution results in a slow increase in reactor power until a DAS reactor trip eventually occurs on a Low SG Level. The dilution will continue, however, until the operator secures CVCS to terminate the event. The applicant reports that it would take approximately 4 hours of continuous maximum rate dilution to erode the available shutdown margin.

The RCCA Ejection accident is analyzed in Technical Report ANP-10304, Section A.3.5.6. Three cases are analyzed. All cases are initiated from the D3 analysis best-estimate full power initial conditions. BOC core conditions are assumed, as the Doppler reactivity feedback mechanism is least effective at BOC. The ejected rod worth of 65 pcm assumed in the D3 analysis is reasonable, considering the values reported in FSAR Tier 2, Section 15.4.8. The applicant reports that the RCCA ejection event assuming no vessel rupture does not exceed the DNBR SAFDL, whereas for the rupture cases the DNBR decreases below the SAFDL. In RAI 413, Question 07.08-31, the staff requested that the applicant provide additional information in order to complete the staff review of the RCCA ejection analysis. In a January 28, 2011, response to Question 07.08-31, the applicant identified the differences in analysis assumptions amongst the RCCA ejection cases and provided a comparison of the key parameters affecting the DNBR calculation. The applicant's response provided the information needed to complete



the staff review. Therefore, the staff finds the January 28, 2011, response to RAI 413, Question 07.08-31 acceptable and considers the issue resolved. In summary, for the Reactivity and Power Distribution Anomalies category of events, the staff finds:

- that the BTP-7-19 best-estimate plant response acceptance criteria are met
- no operator actions are required as a diverse means of protective action

#### *7.8.4.2.5 Increase in RCS Inventory*

The DBEs evaluated in this category of events are:

- Inadvertent Operation of the Safety Injection System or the Extra Borating System (EBS)
- CVCS Malfunction that Increases RCS Inventory

These two events are classified as AOOs. An inadvertent operation of safety injection system assuming Technical Report ANP-10304 analysis nominal full power conditions is not an issue because the safety injection pumps (medium head and low head injection pumps) do not have sufficient pump head to force (deliver) flow into the RCS. However, the EBS utilizes two full capacity positive displacement pumps designed to inject borated water into the RCS at any credible pressure. The PAS pressurizer level control function, which remains operational during a PS SCCF, acts to remove the additional inventory injected by inadvertent operation of both EBS pumps. Therefore, these events are addressed relative to a SCCF in the PS. The CVCS malfunction that increases RCS inventory event, evaluated in Technical Report ANP-10304, Section A.3.6.2 occurs when the CVCS adds coolant to the RCS without letdown, potentially resulting in the pressurizer going solid. The applicant utilizes the results of FSAR Tier 2, Section 15.5.2, non-LOOP CVCS malfunction that increases RCS Inventory analysis to evaluate the pressurizer level response assuming a SWCCF in the PS. The pressurizer is estimated to fill at approximately 24 minutes, assuming CVCS is not isolated, following which the three pressurizer safety relief valves (PSRVs) will relieve pressure. FSAR Tier 2, Revision 2, Section 5.2.2.2.2 confirms the ability of the PSRVs to provide overpressure protection for water solid conditions with RCS letdown isolated. In a March 23, 2011, response to RAI 413, Question 07.08-35, the applicant described a U.S EPR design feature in the PAS which limits the pressurizer level to 70 percent by isolating charging flow. Therefore, overfill of the pressurizer is not possible when the PAS level limitation feature is credited, so no operator actions need be considered. The staff agrees that the level limitation function of the PAS is a reasonable assumption for D3 analyses and that by crediting it no pressurizer overfill will occur. In summary, for the Increase in RCS Inventory category of events, the staff finds:

- SRP BTP-7-19 best-estimate plant response acceptance criteria are met
- There are no operator actions required as a diverse means of protective action

#### 7.8.4.2.6 *Decrease in RCS Inventory*

The DBEs evaluated in this category of events are:

- Inadvertent Opening of a PSRV
- SG Tube Rupture
- Loss-of-Coolant Accidents

The Inadvertent Opening of a PSRV is classified as an AOO and the SGTR and LOCA events are classified as a PAs.

In Technical Report ANP-10304, Section A.3.7.1 the applicant provides an engineering argument that the inadvertent opening of a PSRV event is comparable to FSAR Tier 2, Chapter 15 analysis. The FSAR Tier 2, Chapter 15 analysis shows a PS reactor trip actuation on low pressurizer pressure; a trip which is not part of the DAS. A reactor trip is provided by DAS on low hot leg pressure. Considering the rapid drop in RCS pressure evidenced from FSAR Tier 2, Figure 15.6-2, and the DAS low hot leg pressure trip is approximately 40 psi lower than the PS low pressurizer pressure trip, the difference between the trip time in Technical Report ANP-10304 and FSAR Tier 2, Chapter 15 analyses is insignificant. Therefore, adequate protection is provided during the inadvertent opening of a PSRV with SCCF in the PS.

The SG Tube Rupture event challenges the radiological release limits and poses the potential for SG overfill with water entering the main steam lines. As described in Technical Report ANP-10304, Section A.3.7.2, the same manual actions credited in FSAR Tier 2, Section 15.6.3 analysis are available in the D3 analysis with a SCCF of the PS. The staff verified the availability of the credited actions per Section A.2.2. The radiological results of the D3 SGTR analysis are bounded by FSAR Tier 2, Section 15.6.3 SGTR analysis, due to D3 analysis assumption that the PAS turbine bypass operation is available for cooldown (turbine bypass discharges to the main condenser as opposed to the MSRT discharge directly to atmosphere as assumed in FSAR analysis).

For the SG overfill analysis, FSAR Tier 2, Section 15.6.3, reports that the affected SG does not overfill, as depicted in FSAR Tier 2, Figure 15.6-105. The D3 analysis presented in Technical Report ANP-10304, Section A.3.7.2 reports that the affected SG exceeds 100 percent wide range level and a small amount of liquid discharges into the main steam line. The staff determined the explanation for the SG overfill and the eventual termination of the fill scenario insufficient. Additionally, the applicant's finding that liquid enters the steam line is of concern to the staff because of the potential for steam condensation and water hammer in the steam line. In RAI 413, Question 07.08-32, the staff requested that the applicant address these concerns. In a March 23, 2011, response to RAI 413, Question 07.08-32, the applicant stated that its original evaluation of the SGTR event was made with a simplified engineering evaluation rather than a detailed simulation of the event. The response also provided a comprehensive analysis of the event using S-RELAP5, which has been updated in Technical Report ANP-10304. The applicant's revised analysis of the SGTR event showed that the maximum SG water level was 84 percent of wide range. The SG does not overfill and no liquid enters the steam lines. The staff reviewed that applicant's revised analysis and found the response and the assumptions inherent in it reasonable. Therefore, the staff finds the applicant's March 23, 2011, response to RAI 413, Question 07.08-32 acceptable and considers the question resolved.

The Loss of Coolant Accidents evaluated in Technical Report ANP-10304, Section 3.7.3 include large break (LBLOCA) and small break (SBLOCA) events. FSAR Tier 2, Section 15.6.5.1 analysis, of the LBLOCA does not take credit for a reactor trip. However, an RCP trip on RCP low differential pressure concurrent with SIS actuation signal (FSAR Tier 2, Section 7.3.1.2.15, Interim Revision 3 mark-ups) occurs at about 10 seconds. As described in FSAR Tier 2, Revision 2, Section 5.4.1.3, the RCP trip signal is provided by the PS. Therefore, the RCP trip does not automatically occur for the LBLOCA with a SCCF in the PS. In Technical Report ANP-10304, Section A.3.7.3.1, the applicant states that continued operation of the RCPs during a LBLOCA does not have significant impact on the LBLOCA results. In RAI 413, Question 07.08-33, the staff requested in part that the applicant provide the results of the sensitivity study that provides the basis for their determination of no significant impact. In a February 1, 2011, response to RAI 413, Question 07.08-33, the applicant provided the results of the applicant's sensitivity study. In particular, a plot of cladding temperature response for RCPs tripped and not tripped. Not tripping the RCPs increased the calculated PCT by about 16.7 °C (30 °F) in the D3 analysis. There remains ample margin (several hundred degrees) to the cladding temperature safety limit. The February 1, 2011, response to RAI 413, Question 07.08-33 provided the information requested by the staff and proves the "no significant impact" assertion made by the applicant. Therefore, the staff finds the applicant's February 1, 2011, response to RAI 413, Question 07.08-33 acceptable and considers the question closed.

Technical Report ANP-10304, Section A.3.7.3.1 presents an engineering argument that, because best-estimate core conditions and the availability of all four trains of the SI system in the D3 analysis, the Chapter 15 safety analysis of LBLOCA event remains bounding. In the FSAR analyses, the PS actuates SI on low pressurizer pressure and the DAS also actuates SI on low pressurizer pressure. Therefore, the staff finds the FSAR Chapter 15 bounding for LBLOCA conclusion acceptable. For the SBLOCA, the Chapter 15 safety analysis provided in FSAR Tier 2, Section 15.6.5.2 shows the occurrence of a reactor trip on low pressurizer pressure followed by SI system actuation. For the SBLOCA with SCCF in the PS (Technical Report ANP-10304, Section A.3.7.3.2), a DAS reactor trip occurs on low hot leg pressure followed by SI system actuation. An equivalent level of protection is therefore provided by DAS relative to FSAR Tier 2, Chapter 15 analysis. For the D3 analysis of SBLOCA, as described above for LBLOCA, an RCP trip does not automatically occur. The lack of automatic RCP trip for SBLOCA is not in conformance with Three Mile Island Action Plan requirement II.K.3.5, "Automatic Trip Of Reactor Coolant Pumps During Loss-Of-Coolant Accident," of NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980, as stated in FSAR Tier 2, Sections 15.6.5.2.2 and 15.6.5.2.6. The position of TMI Action Plan requirement II.K.3.5 states, among other things:

Tripping of the reactor coolant pumps in case of a loss-of-coolant accident (LOCA) is not an ideal solution. Licensees should consider other solutions to the small-break LOCA problem (for example, an increase in safety injection flow rate). In the meantime, until a better solution is found, the reactor coolant pumps should be tripped automatically in case of a small-break LOCA. The signals designated to initiate the pump trip are discussed in NUREG-0623.

The staff accepted manual RCP trip for SBLOCA based, for example, on zero degrees hot leg sub-cooling indication. As stated, among other things, in GL No. 85-12 "Implementation of TMI Action Item II.K.3.5, "Automatic Trip of Reactor Coolant Pumps," June 1985:

With regard to the Westinghouse Owners Group (WOG) submittals referenced in Section V of the enclosed Safety Evaluation, we conclude that the methods

employed by the WOG to justify manual reactor coolant pump (RCP) trip are consistent with the guidelines and criteria provided in Generic Letters 83-10 c and d. The approved Westinghouse Small Break LOCA Evaluation Model was used to demonstrate compliance with 10 CFR 50.46 and Appendix K to 10 CFR Part 50. We have determined that the information provided by the WOG in support of the alternative RCP trip criteria is acceptable on a generic basis.

The selection is based upon obtaining maximum discrimination between a small break LOCA (which requires RCP trip) and a SG tube rupture (which does not require RCP trip). In reviewing the WOG RCP trip criteria, we note that the process of criterion selection involves a number of considerations which were assigned plant-specific status by the WOG during the process of the trip criteria review.

As discussed in Technical Report ANP-10304, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," Revision 4, the applicant performed SBLOCA sensitivity studies to determine the latest RCP manual trip time utilizing D3 best-estimate analysis assumptions. This included addressing the availability of all four trains of SI system, and demonstrated that the maximum peak cladding temperature (PCT) for SBLOCA would remain well within the 10 CFR 50.46 acceptance criteria even if the RCPs are not tripped. From the results of the sensitivity studies, the applicant concluded that, "the analyses also demonstrate that an RCP trip during an SBLOCA event with an SCCF in the PS is not needed to mitigate the event and therefore, operator criteria or a D3 coping procedure for tripping the RCPs during this event are not necessary." However, staff notes that the applicant also states in Technical Report ANP-10304

During an SBLOCA with RCPs running, a greater amount of inventory could be lost out the break than with RCPs tripped. After sufficient inventory is lost and the RCPs are tripped, a deeper core uncover could result in a higher PCT. DAS does not include an [automatic] RCP trip function. With an SWCCF in the PS, the RCPs continue operating, with the opportunity to be tripped (manually) at a later time.

The staff finds that a RCP trip during SBLOCA may be preferable in order to reduce inventory loss out the break and preserve operability of the RCPs. Therefore, the staff concludes that a credited diverse manual (versus DAS automatic) RCP trip should be included within the credited diverse D3 manual controls inventory. However, the staff was not able to identify a manual D3 RCP Trip as a credited D3 manual actuations available to the operator on SICS. Therefore, in follow-up RAI 505, Question 07.08-44, the staff requested that the applicant clarify the D3 RCP Reactor Trip issue. **RAI 505, Question 07.08-44 is being tracked as an open item.**

The issue of RCP trip for SBLOCA is addressed further in the operator manual actions evaluation review in Section 7.8.4.1.3 of this report. RCS depressurization following a SBLOCA may be accomplished via the MSRT partial cooldown function actuated through the PS. In the absence of a PS signal, the Turbine Bypass System (TBS), through PAS, is capable of performing the cooldown function, provided the MSIVs remain open. In a February 1, 2011, response to RAI 413, Question 07.08-34, the applicant addressed the staff's concern that the TBS might not be available during a SBLOCA. The response provided an analysis which showed that it is not necessary to rely on the TBS for partial cooldown during a SBLOCA with a SCCF in the PS. The staff reviewed the applicant's analysis and finds that it provides reasonable assurance that any SBLOCA can be brought under control and the reactor safely

brought to cold shutdown without relying on manual or automatic activation of the TBS. Therefore, the staff finds the applicant's February 1, 2011, response to RAI 413, Question 07.08-34 acceptable and, therefore, consider this issue resolved. In summary, upon satisfactory closure of RAI 505, Question 07.08-44 for the Decrease in RCS Inventory category of events, the staff finds:

- SRP BTP 7-19 best-estimate plant response acceptance criteria are met
- no operator actions are required as a diverse means of protective action

#### *7.8.4.2.7 Containment Integrity*

The D3 analysis criterion for meeting containment structure integrity is the ultimate pressure capacity. The design basis containment analysis is presented in FSAR Tier 2, Revision 2, Section 6.2.1. The limiting events, based on FSAR Tier 2, Revision 2, Chapter 6, "Engineered Safety Features," containment mass and energy release analyses, are the LBLOCA and MSLB accidents. Based on FSAR Tier 2, Section 6.2.1, containment analysis of the inside-containment LBLOCA, the limiting case at full power is a hot leg double-ended guillotine break, resulting in a blow-down peak containment pressure of 0.46 MPa (52 psig) occurring at about 31 seconds into the transient; thus remaining below the containment design pressure of 0.53 MPa (62 psig). Considering a LBLOCA with a concurrent SCCF in the PS, the same RT and SI system functions provide protective action (though slightly delayed due to lower DAS setpoints), and the mass and energy releases will be similar to those described in FSAR Tier 2, Chapter 6. Further, assuming D3 best-estimate assumptions (i.e., nominal full power, per FSAR Tier 2, Sections 6.2.1.3.1, Revision 2) versus the conservative assumptions (i.e., conservatively high fuel temperatures, per FSAR Tier 2, Revision 2, Section 6.2.1.3.2), it is reasonable to conclude that containment structure integrity will be maintained in the event of an inside-containment LBLOCA with a concurrent SCCF in the PS.

FSAR Tier 2, Revision 2, Section 6.2.1, containment analysis of the MSLB at full power conditions shows that the calculated peak containment pressure of 0.45 MPa (50.52 psig) occurs at about 47 seconds into the transient and remains below the containment design pressure of 0.53 MPa (62 psig). The staff also finds also that although the calculated vapor temperature exceeds the containment design value of 170 °C (338 °F), the actual containment wall temperature will be near saturation, which is well below the containment design. For the case of a MSLB with SCCF in the PS, the same MFW and MSL isolation functions are available as compared to the safety analysis (though slightly delayed due to lower DAS setpoints). Considering the use of best-estimate assumptions versus the conservative assumptions, it is reasonable to conclude that containment structure integrity will be maintained. Based on the above evaluations, the staff finds that Technical Report ANP-10304 analysis criterion on containment structure integrity is met.

#### *7.8.4.2.8 Radiological Consequences*

Technical Report ANP-10304, Section A.3.9 addresses the radiological consequences of the limiting events identified in FSAR Tier 2, Section 15.0.3, consistent with NUREG-0800, Section 15.0.1, including: Small line break outside containment; LOCA; SGTR; MSLB; RCP Rotor Seizure; RCCA Ejection; and Fuel Handling Accident. The staff notes that Technical Report ANP-10304, Section A.3.9 lists the feedwater line break for radiological consequence evaluation, although feedwater line break is not addressed in either SRP, Section 15.0.1 or FSAR Tier 2, Section 15.0.3. However, the feedwater line break is bounded by the MSLB relative to potential fuel damage (FSAR Tier 2, Section 15.2.8.6).

For inside containment release events (LOCA, MSLB, RCCA Ejection), DAS provides the containment isolation function credited in FSAR Tier 2, Chapter 15 analysis (though slightly delayed due to higher DAS setpoint), to limit offsite dose consequences. Considering the use of best-estimate assumptions for the D3 analyses versus the conservative assumptions (e.g., LOOP, reactor coolant iodine and noble gas activity levels at plant Technical Specification limits, conservative iodine spiking factor, and bounding failed fuel fractions per FSAR Tier 2, Section 15.0.3.3), the radiological consequences are expected to meet the D3 acceptance criteria.

The events that result in radiological release outside of containment are small line break, SGTR, MSLB, Fuel Handling Accident, and RCP Rotor Seizure. The small line break does not cause fuel failure, and since FSAR Tier 2, Section 15.0.3.5.1 analysis, of the small line break conservatively assumes iodine and noble gas activity levels at plant Technical Specification limits, the D3 analysis is bounded by FSAR Tier 2, Chapter 15 analysis. Similarly for SGTR event, the FSAR analysis bounds the D3 analysis.

The D3 analysis of MSLB in Technical Report ANP-10304, Section A.3.2.5 reports that no fuel failure occurs and, therefore, FSAR Tier 2, Section 15.0.3.7 analysis of the radiological consequences of the MSLB accident remain bounding.

The Fuel handling Accident (classified as a PA) does not involve a reactor trip and considering the conservative assumptions used in FSAR Tier 2, Section 15.0.3.10 analysis, FSAR analysis remains bounding.

FSAR Tier 2, Section 15.0.3.8, reports that the radiological dose acceptance criteria may be met for a RCP Rotor Seizure accident with up to 9.5 percent fuel failures. FSAR Tier 2, Section 15.3.3, states that approximately 8 percent of the fuel is calculated to fail as a result of the RCP Rotor Seizure accident. Considering the conservative FSAR assumptions (coincident LOOP, stuck open MSRT valve to atmosphere, loss of one of two divisions of control room charcoal filtration systems, pre-accident iodine spike), the D3 radiological analysis of the RCP Rotor Seizure accident is bounded by FSAR Tier 2, Section 15.0.3.8 analysis. Based on the above evaluations, the staff finds that the BTP 7-19 best-estimate D3 plant response acceptance criteria on radiological consequences are met.

#### 7.8.4.3 *ATWS Mitigation*

An ATWS event is defined as an AOO followed by the failure of the reactor trip portion of the protection system. The ATWS definition is based on the failure of the control rod trip system (reactor trip portion) to insert the rods into the core upon protection system initiation. An applicant's proposed ATWS mitigation system is required to automatically initiate turbine trip, emergency (or auxiliary) feedwater, and, depending on pressurized water reactor manufacturer, scram the reactor. This ATWS system is required to be diverse from the existing reactor trip system. Technical Report ANP-10304, Section A.1 states that the ATWS mitigation system for the U.S. EPR is the DAS.

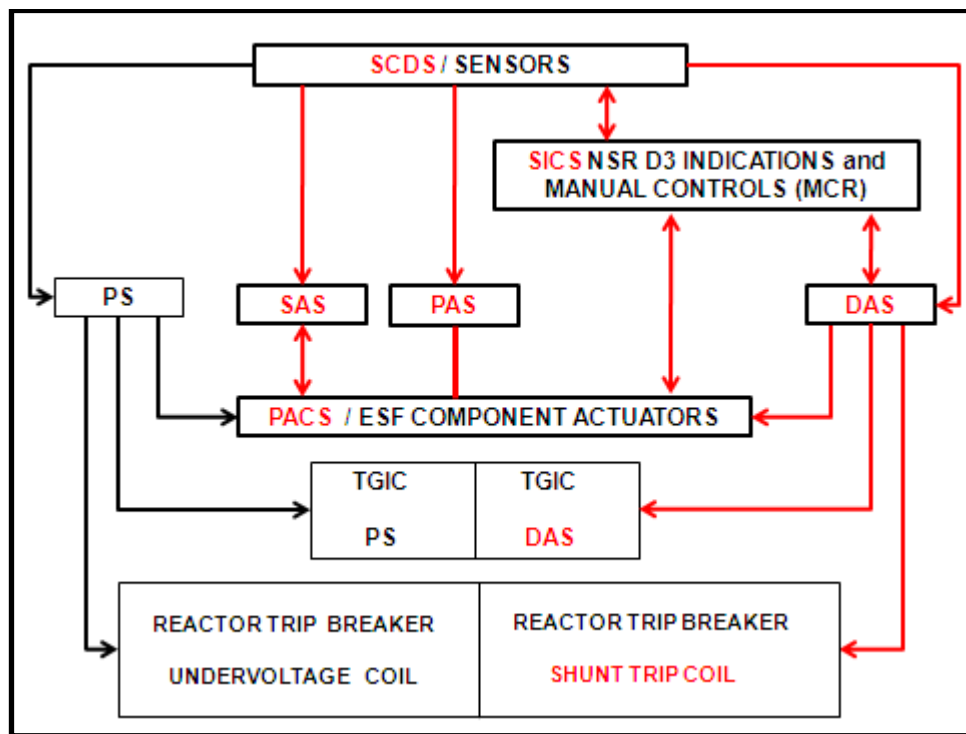
FSAR Tier 2, Section 7.8.2.1.3, Interim Revision 3 mark-ups, states that the DAS, SCDS, and PACS are provided for ATWS mitigation. DAS automatically initiates RT, turbine trip, and EFW on conditions indicative of an ATWS. FSAR Tier 2, Figure 7.8-9 of the Interim Revision 3 mark-ups displays the ATWS mitigation systems. Items in red are the credited ATWS mitigation systems, which include SCDS, PAS, DAS, PACS, and the reactor trip breaker shunt trip coil.

As stated in FSAR Tier 2, Section 7.8.1.1.3, Interim Revision 3 mark-ups, and Technical Report ANP-10304, Section 3.2.1.1, the PS reactor trip outputs are de-energized to actuate a reactor trip. The diverse means to initiate a reactor trip is an initiation signal from the DAS. FSAR Tier 2, Sections 7.1.1.5.1, 7.7.1.1 and 7.8.1.1.3, Interim Revision 3 mark-ups, and Technical Report ANP-10304, Section 3.2.1.1 state that CRDCS contains rod control units that are diverse from the reactor trip breakers and reactor trip contactors which generates and sends control rod movement (i.e., withdrawal, insertion, hold) signals to the CRDCS coil modules to control rod movement. To initiate a diverse trip from the PS, the DAS sends a control rod drop signal (energized to initiate) to interrupt power to the CRDCS rod control units. In addition, the reactor trip breakers consist of a shunt trip coil which is diverse from the PS undervoltage coil. Control rod trip outputs from the DAS are also sent to the shunt trip coils of the RT breakers, which are a diverse means of opening the breakers from the reactor trip undervoltage coils, which are controlled by the PS.

FSAR Tier 2, Section 7.8.2.1.3, Interim Revision 3 mark-ups, states that the DAS automatically initiates reactor trip, turbine trip, and EFW actuation on conditions indicative of an ATWS. For DAS diverse EFW actuations (and applicable diverse credited ESF actuations), actuation output signals from the DAS are sent directly to the PACS by hardwired connections. DAS actuation signal outputs to initiate turbine trip are sent directly to the turbine generator I&C by a hardwired connection as well. Neither of these DAS diverse signal paths are affected by a postulated SCCF of the PS because both bypass the PS processing components and are connected directly to the PACS or the turbine I&C controls, whichever is applicable.

The staff's findings for the complete diverse ATWS and D3 mitigation I&C systems is illustrated in Figure 7.8-4 below.

**Figure 7.8-4 ATWS / D3 Mitigation Systems<sup>8</sup>**



Note: NSR – non-safety related.

#### 7.8.4.4 *Manual Actions for D3*

To address Point 3 of the NRC four point D3 policy stated in the SRM to SECY-93-087, Item II.Q, for disabled safety functions due to a CCF of the primary PS, the D3 design shall provide a “diverse means” to perform either the same function or a different function. The staff’s position, as stated in ISG-02, Section 1, states:

When an independent and diverse method is needed as backup to an automated system used to accomplish a required safety function, the backup function can be accomplished via either an automated system, or manual operator actions performed in the main control room.

Therefore, the applicant can credit manual operator actions, performed from the MCR, as a diverse means to perform the safety function that would have been performed by the failed primary PS. Upon the staff’s review of the applicant’s D3 plant response provided in Technical Report ANP-10304 and design information provided in FSAR Tier 2, Section 7.8, Interim

<sup>8</sup> Generated from Technical Report ANP-10304 Figure 2-1, Figure 4-1, and Figure 4-2; and U.S. EPR FSAR Tier 2, Figure 7.1-27, Interim Revision 3 mark-ups



Revision 3 mark-ups, the staff could not identify any manual operator actions that were credited as a diverse means to perform failed safety functions as required by Point 3 of the NRC's D3 policy.

Therefore the staff found that FSAR Tier 2, Chapter 15 safety analyses, credit operator actions as necessary to mitigate design basis events and that many of D3 analyses presented in Technical Report ANP-10304, Appendix A, assume the same operator actions taken in FSAR Tier 2, Chapter 15 analyses. However, additional operator actions are credited in response to an event with SCCF in the PS. The staff reviewed each of the D3 analysis events and identified 28 instances where operator action is credited. With the exception of the manual RCP trip identified in Technical Report ANP-10304, Section A.3.7.3.2, the operator actions listed in Technical Report ANP-10304, Section A.1 correctly represent all the operator actions cited in the individual Appendix A plant response analysis sections of Technical Report ANP-10304. Technical Report ANP-10304, Table A.2-1 identifies the credited manual operator actions. The following is a summary of several manual actions regarding the D3 analysis.

For the Decrease in Feedwater Temperature event, manual control of EFW after one hour for decay heat removal is not considered a required D3 diverse means.

The D3 analysis of the Increase in Steam Flow event states that the operator terminates the transient at some point, but the analysis indicates that an RT is not necessary. The manual RT, therefore, is not considered a required D3 diverse means. For the same initiating event, but assuming RT on low SG level, EFW will actuate and require operator control. Operator control of feedwater for long-term cooling is not considered a required D3 diverse means.

The D3 analysis of the Loss of AC to Station Auxiliaries event states that the EDGs must be manually started and loaded, or the SBO DGs must be loaded manually (following automatic start of SBO DGs by the DAS) in order to power the EFW pumps for restoration of feedwater. The applicant calculates that the SGs will boil dry in about 1 ½ hours. The staff expressed concern that operator action to start the EDGs and load the EFW pumps to either the EDGs or SBO DGs might represent a required D3 diverse means. In a February 1, 2011, response to RAI 413, Question 0708-25, the applicant adequately addressed the staff's concern. The response stated that even if the EFW pumps could not be started within 1 ½ hours, the operator could initiate a feed and bleed procedure to control RCS pressure. The staff finds the February 1, 2011, response to RAI 413, Question 07.08-25 acceptable and, therefore, considers this question resolved. Operator control of EFW within 1½ hours is not considered a required D3 diverse means.

For the FW line break accident, the manual control of MSRTs for long-term decay heat removal is not considered a required D3 diverse means.

The Boron Dilution event described in Technical Report ANP-10304, Section A.3.5.5 states that in the absence of ADM (requires input from PS), the operator is calculated to have approximately 4 hours to terminate the transient before shutdown margin is lost. The operator action is considered reasonable and is expected to be covered by plant abnormal operating procedures or emergency operating procedures. No special manual D3 diverse means are deemed necessary to mitigate this event.

For the Increase in RCS Inventory event, the transient does not terminate on pressurizer high level as is the case with FSAR Tier 2, Chapter 15 analysis. In the Chapter 15 analysis, the pressurizer high level causes a RT and CVCS isolation. For the D3 analysis, neither the RT, nor the CVCS isolation occurs, and the pressurizer fills solid. Although Technical Report

ANP-10304, Section A.3.6.2 states that PSRVs are capable of relieving water, thus ensuring that the RCS pressure boundary is maintained, sufficient indication and procedures should be available to ensure that the operators recognize and terminate the event in a timely manner. In a March 23, 2011, response to RAI 413, Question 07.08-35, the applicant described a design feature in the PAS which limits the pressurizer level to 70 percent by isolating charging flow. Overfill of the pressurizer is not possible when the PAS level limitation feature is credited, so no operator actions (i.e., diverse means) need be considered. The staff finds that crediting the level limitation function of the diverse PAS acceptable for D3 analyses and that by crediting it no pressurizer overfill will occur.

Technical Report ANP-10304, Section 3.7.3.2 states that during a SBLOCA, the RCPs continue to operate and that the operator has the opportunity to trip the RCPs at a later time. While the applicant's sensitivity studies (see above SBLOCA evaluation) demonstrate that RCP trip is not required to meet the 10 CFR 50.46 acceptance criteria, RCP trip during SBLOCA may be preferable in order to reduce inventory loss out the break and preserve operability of the RCPs. The staff requested the applicant in RAI 413, Question 07.08-36, to provide additional information relative to RCP trip during SBLOCA with SWCCF in the PS for:

- a. The criteria for operator determination of the need for RCP trip, i.e., LOCA as confirmed by two-phase RCS flow conditions,
- b. The displays available to the main control room operators to determine the need for RCP trip, and
- c. Identification of the procedure or procedure type (e.g., EPGs) that will prescribe the steps to accomplish the required operator action and whether a special D3 coping procedure is required.

In a January 28, 2011, response to RAI 413, Question 07.08-36, the applicant clarified that neither operator action criteria, nor a D3 coping procedure for tripping the RCPs during a SBLOCA are necessary. In addition, the applicant revised Technical Report ANP-10304, Section 3.7.3.2 to include an expanded description of the evaluation of the effect of RCP trip on SBLOCA simulations. The staff finds that the revision adequately addressed the absence of a RCP trip during a SBLOCA and, therefore, considers the January 28, 2011, response to RAI 413, Question 07.08-36 acceptable and consider this question resolved.

For the radiological consequences of accidents concurrent with a SCCF in the PS, Technical Report ANP-10304, Section A.3.9 states that DAS does not provide automatic control room isolation. However, analyses performed by the applicant, however, indicate that manual isolation of the main control room should take place within 30 minutes of an event initiation. Therefore manual isolation of the main control room may represent a required manual D3 diverse means. The staff requested the applicant in RAI 413, 07.08-37, to provide information to justify that manual isolation of the main control room as described in Section A.3.9 of ANP-10304, will occur in a timely manner. In a January 28, 2011, response to RAI 413, Question 07.08-37, the applicant described that, in the event of loss of the PS, the MCR high radiation air intake alarms would sound within five minutes of a radiation release and would alert the operator to isolate the MCR. Isolation would occur within 30 minutes of the alarm signal. The response further explained, while emergency operating procedures are not yet developed for the U.S. EPR, it is anticipated that either abnormal or emergency operating procedures will include instructions for responding to high radiation at the MCR intakes. The staff finds the applicant's description of operator notification of the need for MCR isolation and subsequent

response time to be reasonable. Therefore, the staff finds the January 28, 2011, response to RAI 413, Question 07.08-37 acceptable and consider this question resolved.

Based on the above review, the following operator actions credited in the D3 analysis may be considered a diverse means of protective action to ensure the D3 analysis criteria are met:

- Manual start of and loading of EDGs and/or manual loading of SBO DGs followed by initiation of EFW pumps in response to a Loss of Non-Emergency AC Power to Station Auxiliaries event
- Manual isolation of the main control room in response to a Loss of Non-Emergency AC Power to Station Auxiliaries event

The guidance of DI&C ISG-02, Section 1, states that if manual operator actions are used as backup (i.e., diverse means), a suitable human factors engineering (HFE) analysis should be performed to demonstrate that plant conditions can be maintained within the SRP BTP 7-19-recommended acceptance criteria for the particular AOO or PA. DI&C ISG-02 further states:

The applicant should demonstrate through a suitable HFE analysis that manual operator actions that can be performed inside the control room are acceptable in lieu of automated backup functions.

The staff position in DI&C ISG-05, Section 3, states that a D3 analysis should include the justification of any operator actions that are credited for response to an AOO/PA concurrent with a SCCF. To demonstrate that the manual actions are both feasible and reliable, and that the ability to perform the actions reliably within the time available is maintained, the applicant should follow a process of analysis, validation, and long-term monitoring consistent with the methods presented in DI&C ISG-05. The guidance of DI&C ISG-05, Section 3, also states that the applicant should commit, in the D3 analysis submittal, to include the proposed D3 coping actions in a HFE Program consistent with that described in NUREG-0711 and to provide the results of the HFE Program to the staff prior to implementation of the proposed action(s).

FSAR Tier 2, Section 7.8.1.2.3, Interim Revision 3 mark-ups, states that credited diverse manual functions are subject to evaluation and design per the HFE engineering program described in FSAR Tier 2, Revision 2, Chapter 18, and that all of the manual actions are analyzed during task analysis as described in FSAR Tier 2, Section 18.4.2, Revision 2. The actions are included in the population of human actions that are subject to task support verification and integrated system validation as described in FSAR Tier 2, Revision 2, Sections 18.10.3.1, 18.10.3.3, and 18.10.3.6. The guidance of SRP Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-In-Depth (D3) Analyses," supersedes, and incorporates with limited modifications, the guidance contained in ISG-05, Section 3. SRP Appendix 18-A provides guidance for a methodology that provides early feedback in the design and regulatory review process and allows the applicant to move forward with relative confidence that credited manual operator actions will be demonstrated as both feasible and reliable in the integrated system validation. SRP Appendix 18-A, Section 4.B, states that the ability to reliably perform credited manual operator actions will be verified through completion of license conditions related to the actions credited in the D3 analyses and that the ability to reliably perform the credited manual actions within the time available shall be maintained through a long-term monitoring strategy.

FSAR Tier 2, Revision 2, Section 18.1.1.2 states that the HFE design process addresses the applicable review criteria specified in NUREG-0711. FSAR Tier 2, Revision 2, Section 18.11.1 states that the U.S. EPR design implementation is completed after construction is complete, but before plant startup and that design implementation verifies, among other things, that modifications to the standard U.S. EPR design conform to the HFE principles and design guidance expressed in the HFE style guide and meets the HFE review criteria in NUREG-0711. The staff's review of the HFE program is evaluated in Chapter 18 of this report.

SRP Section 7.8 guidance states that the performance requirements for which credit is taken in the mitigation of design basis events (e.g., dynamic response, accuracy) should be identified. FSAR Tier 1, Revision 2, Table 3.4-1, ITAAC Item 11.0, "Acceptance Criteria," states that an output summary report exists which:

- Demonstrates that the V&V was performed in accordance with the prescribed process
- Demonstrates that the design conforms to HFE design principles
- Demonstrates that the design enables plant personnel to successfully perform their tasks to achieve plant safety and other operation goals
- Provides results of V&V activities and conclusions from these activities

Accordingly, the staff finds that the stated performance requirements response conformance will be confirmed by validation testing, and the commitment addresses the SRP 7.8 guidance for identification of D3 system performance requirements.

Based on the applicant's stated inventory of manual actuation capability from the MCR, the staff finds that the D3 manual actions include the capability for initiation from the MCR, and thus, address the manual initiation capability guidance of SRP Section 7.8.

#### *7.8.4.5 Independence Between Diverse I&C Systems*

##### *7.8.4.5.1 Diverse Power Supplies*

10 CFR 50.62 requires that ATWS equipment be independent from the existing reactor trip system. The guidance of SRP Section 7.8 states that logic and actuation device power for the ATWS mitigation system should be from an instrument power supply independent from the power supplies for the existing RTS. The staff's technical evaluation for the U.S. EPR data communication systems reliability is included in Section 7.9.4.2 of this report.

FSAR Tier 2, Section 7.1.1.4.7, Interim Revision 3 mark-ups, states that the DAS is powered from the 12-hour uninterruptible power supply. FSAR Tier 2, Section 7.1.1.4.6 states that the PAS is powered from the 12-UPS and the non-Class 1E uninterruptible power supply (NUPS). FSAR Tier 2, Section 7.1.1.4.1, states that the PS is powered from the EUPS. FSAR Tier 2, Revision 2, Sections 8.1.1 and 8.1.2 state that the Class 1E EUPS is powered from the transmission system to two emergency auxiliary transformers. It also states that two normal auxiliary transformers provide power from the switchyard to the non-Class 1E 12-UPS and NUPS. Therefore, the staff's review confirmed that power supply between the DAS and PAS comes from an independent source than the PS. Accordingly, staff finds that this diverse power supply design between the DAS, PAS, and the PS, meets the diverse independence guidance of SRP Section 7.8

FSAR Tier 2, Section 7.1.1.4.2, Interim Revision 3 mark-ups, states that the SAS is powered from EUPS. FSAR Tier 2, Section 7.1.1.3.1 states that the safety-related portion of the SICS is powered from the EUPS and that the non-safety-related portion of the SICS is powered from the 12-UPS. The staff finds that the power supply between the SAS and safety-related portion of the SICS comes from the same power source as the PS. The staff's review did find that the non-safety-related portion of the SICS power supply comes from an independent power supply other than the PS. Furthermore, the credited D3 information and manual control actuations are performed from the DAS indications and controls that are located on the non-safety-related portions of the SICS. Accordingly, staff finds that this diverse power supply design between the non-safety-related portion of the SICS and the PS address the diverse independence guidance of SRP Section 7.8

#### *7.8.4.5.2 Diverse I&C System Interconnections*

10 CFR 50.62 requires that ATWS equipment must be independent and diverse (from sensor output to the final actuation device) from the existing reactor trip system. GDC 24 requires that the protection system shall be separated from control systems to the extent that failure of any single control system component or channel, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system and that interconnections of the protection and control systems shall be limited so as to assure that safety is not significantly impaired. The staff used the guidance in SRP BTP 7-19, Section B.3, to evaluate the independence between the credited D3 I&C systems and the safety I&C systems.

The staff identified several D3 credited control system and PS interconnections and possible design vulnerabilities and evaluated each for conformance to the applicable guidance and requirements. The staff's evaluation will focus on the D3 diverse mitigation systems displayed in the block diagram of Figure 07.08-4 of this report.

The top of Figure 07.08-4 of this report shows that the sensor inputs are common interconnections between the PS and the diverse PAS and DAS. The system credited to distribute sensor inputs to all three systems is the SCDS. FSAR Tier 2, Figure 7.1-23, Interim Revision 3 mark-Ups, provides a block representation of the SCDS system for one division.

FSAR Tier 2, Section 7.1.1.4.8, Interim Revision 3 mark-ups, states that the SCDS is composed of safety-related and non-safety-related equipment, per division. The safety-related SCDS and non-safety-related SCDS equipment is located in separate cabinets. The SCDS is composed of non-computerized signal conditioning modules and signal distribution modules that are part of the TXS platform. The SCDS receives hardwired signal inputs from sensors or black boxes. Sensor information is acquired by the DAS from the SCDS using a hardwired signal path. The SCDS sends hardwired signal outputs to the SICS, DAS, PS, SAS, RCSL, and PAS, as needed. FSAR Tier 2, Section 7.8.1.1.5, states that the outputs of the SCDS are hardwired and are sent independently to each system. The SCDS is also connected directly to the SICS using a hardwired signal path that bypasses the PS for the credited D3 diverse display of sensor information. The SCDS outputs from safety-related SCDS equipment to non-safety-related I&C systems are electrically isolated by the signal distribution modules. SRP BTP 7-11 provides guidance for the use of electrical isolation devices to allow connections between safety and non-safety systems. SRP BTP-7-11 deals with the criteria and methods used to confirm that the design of isolation devices assures that credible failures in the connected non-safety-related systems and channels will not prevent the safety systems from meeting their required protective functions. In addition, RG 1.75, "Criteria for Independence of Electrical Safety Systems," endorses IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment

and Circuits,” which identifies specific electrical isolation criteria for isolation devices used in I&C circuits. In RAI 442, Question 07.01-26, the staff requested that the applicant provide additional design details of the SCDS. In a June 22, 2011, response to RAI 442, Question 07.01-26, the applicant stated, in part, that the SCDS does not share signals between divisions and that the SCDS does not use interdivisional communication.

The staff’s review of the SCDS system requirements, as listed in FSAR Tier 2, Table 7.1-2, finds that the applicant commits to designing the SCDS qualified isolation devices to the guidance of RG 1.75, BTP 7-11, and IEEE Std 384-1992. In addition, FSAR Tier 2, Figure 7.1-23, Interim Revision 3 mark-up, shows that the DAS and PAS safety-related SCDS connections are electrically isolated by qualified isolation devices. The staff’s review also concluded that since the SCDS safety-related equipment is placed in separate cabinets, then postulated failures of the non-safety-related equipment will not degrade the safety-related SCDS equipment’s functionality. Technical Report ANP-10304, Section 4.2 states that the SCDS design does not perform any automatic actuation functions designed to mitigate AOOs or PAs. In addition, Technical Report ANP-10304, Section 4.2 also states that the distribution functions performed by the SCDS are done by either electronic modules or programmable electronic modules that are not based on microprocessors and that there is no software running in the SCDS. Therefore, the SCDS equipment would not be susceptible to a postulated SCCF. The staff also finds that the SCDS non-safety-related equipment is independent from the PS due to the separate and independent power supplies. Based on SCDS different design purpose, equipment, and functionality, the staff finds that the SCDS is adequately diverse and independent from the PS.

Postulated safety-related SCDS failures, or removal from service, would not affect the D3 design due to the fact that SCDS outputs to DAS and PAS are provided in both the safety-related and the non-safety-related SCDS equipment. Postulated non-safety-related SCDS system failures would not impair the trip function and/or ESF functionality of the PS. Therefore, staff finds that the reliability, redundancy, and independence requirements of the protection system would not be degraded due to a non-safety-related SCDS component or channel failure. Additional discussion on independence between U.S. EPR I&C systems is found in Section 7.1.4.10 of this report.

#### 7.8.4.5.2.1 Priority and Actuation Control System Interconnections

The system credited to prioritize component actuation requests from safety-related and non-safety-related systems I&C systems is the PACS. FSAR Tier 2, Figure 7.1-8, Interim Revision 3 mark-ups provides a diagram of the PACS. As described in Technical Report ANP-10310, “Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report,” Revision 1, the safety-related portion of the PACS uses an electronic module where the logic that performs the prioritization control and command termination are implemented that is a PLD. FSAR Tier 2, Section 7.1.1.6.5, Interim Revision 3 mark-ups, states that the PACS design allows for multiple I&C systems to send requests to a given actuator. Priority logic within the PLD dictates that in case of conflicting orders between the PS and the DAS, the PS orders have a higher priority. The diverse non-safety-related DAS is given a higher priority than the safety-related SAS because the applicant states that the DAS is a functional substitute for the PS (both compare sensor inputs to setpoints threshold values to automatically initiate plant protective functions and mitigation actions).

DI&C ISG-02), Section 5 states that there are two possible design attributes that are sufficient to eliminate consideration of a SCCF. The first design attribute is diversity, where the

safety-related protection system contains sufficient diversity within itself (e.g., two divisions are sufficiently diverse from the other two divisions). The second design attribute is testability, where the system is sufficiently simple such that every possible combination of inputs, internal and external initial states, and every signal path can be tested (i.e., the system is exhaustively tested). DI&C ISG 04, Section 2 provides staff guidance regarding the design attribute of testability.

In Technical Report ANP-10310, the applicant proposes a PACS design that follows the staff guidance described in DI&C ISG-02 and ISG-04 with regards to testability. In other words, the applicant commits to (1) describe the testing methodology for 100 percent combinatorial testing that will be applied to the PACS's priority modules and (2) will demonstrate that the submitted methodology for 100 percent combinatorial testing of the priority module conforms to the applicable guidance in ISG-04 for proof-of-concept testing. FSAR Tier 1, Section 4.10, Interim Revision 3 mark-ups, states that the capability of 100 percent combinatorial testing of the PACS priority module is provided to preclude a SCCF. FSAR Tier 2, Section 7.1.1.4.4, Interim Revision 3 mark-ups, states that a diversity requirement for the PACS is that PACS priority modules must be 100 percent tested to eliminate consideration of SCCF. FSAR Tier 1, Table 2.4.5-3, Interim Revision 3 mark-ups, ITAAC Acceptance Criteria Item 4.10, states that a report will exist and conclude that 100 percent combinatorial type testing on the PACS priority module has been successfully completed. Accordingly, the staff did not require a demonstration of the D3 plant response conformance to the guidance of SRP BTP 7-19 for a postulated CCF of the PACS priority module. Further discussion of the staff's review of PACS, including the 100 percent combinatorial testing, independence, redundancy, and other design aspects, is found in Section 7.1 of this report. Based on the applicant's commitment to 100 percent combinatorial testing of the PACS, as allowed by DI&C ISG-02 and ISG-04, the staff finds that the PACS does not need to be considered for a postulated SCCF within the applicant's D3 analysis. The 100 percent combinatorial testing demonstrates sufficient quality of the logic such that a SCCF of the device would be of a sufficiently low frequency that it would not need to be considered in the D3 design.

#### 7.8.4.5.2.2 Turbine Generator I&C System Interconnections

The TG I&C system is another common interconnection between the PS and the DAS. FSAR Tier 2, Section 7.1.1.5.13 states that the TG I&C system performs a turbine trip when requested by either the PS or DAS. As displayed in FSAR Tier 2, Figure 7.1-27, Interim Revision 3 mark-ups, the DAS hardwired inputs to the TG I&C system are separate and independent from the PS hardwired inputs. As shown on Technical Report ANP-10304, Figure 2-1 and as stated in Technical Report ANP-10309, Revision 3, Section 12.1 information is transferred from the PS to the TG I&C system for the turbine trip function via an isolated, hardwired connection. The design requirements for the PS, as stated in FSAR Tier 2, Table 7.1-2, identify that the PS will be designed to the electrical qualification requirements of RG 1.75, BTP 7-11, and IEEE Std 384-1992. Postulated failure of DAS control signals and TG I&C control system would not affect PS functionality and would leave intact a PS that continues to satisfy all reliability, redundancy, and independence requirements of the PS. Therefore, the staff finds that the TG I&C is considered a final actuation device for addressing 10 CFR 50.62 and there is sufficient independence between PS and DAS with regards to the TG I&C connection.

#### 7.8.4.5.2.3 Reactor Trip Breaker Interconnections

At the bottom of Figure 07.08-4 of this report is displayed another interconnection between the PS and the diverse DAS at the reactor trip breakers. The staff evaluation of the adequate

diversity, independence, and separation of the PS and DAS interconnections at the RTBs is discussed in Section 7.8.4.1.1 of this report.

#### 7.8.4.6 *Evaluation of Safety I&C System Vulnerabilities*

The guidance of NUREG/CR-6303 states that the analysis of defense-in-depth should be performed by postulating concurrent failures of the same block or identical blocks in all redundant divisions. It also states that postulated failures within the block fail all block output signals and that these failed block output signals must be assumed to fail in a manner that is credible but that produces the most detrimental consequences.

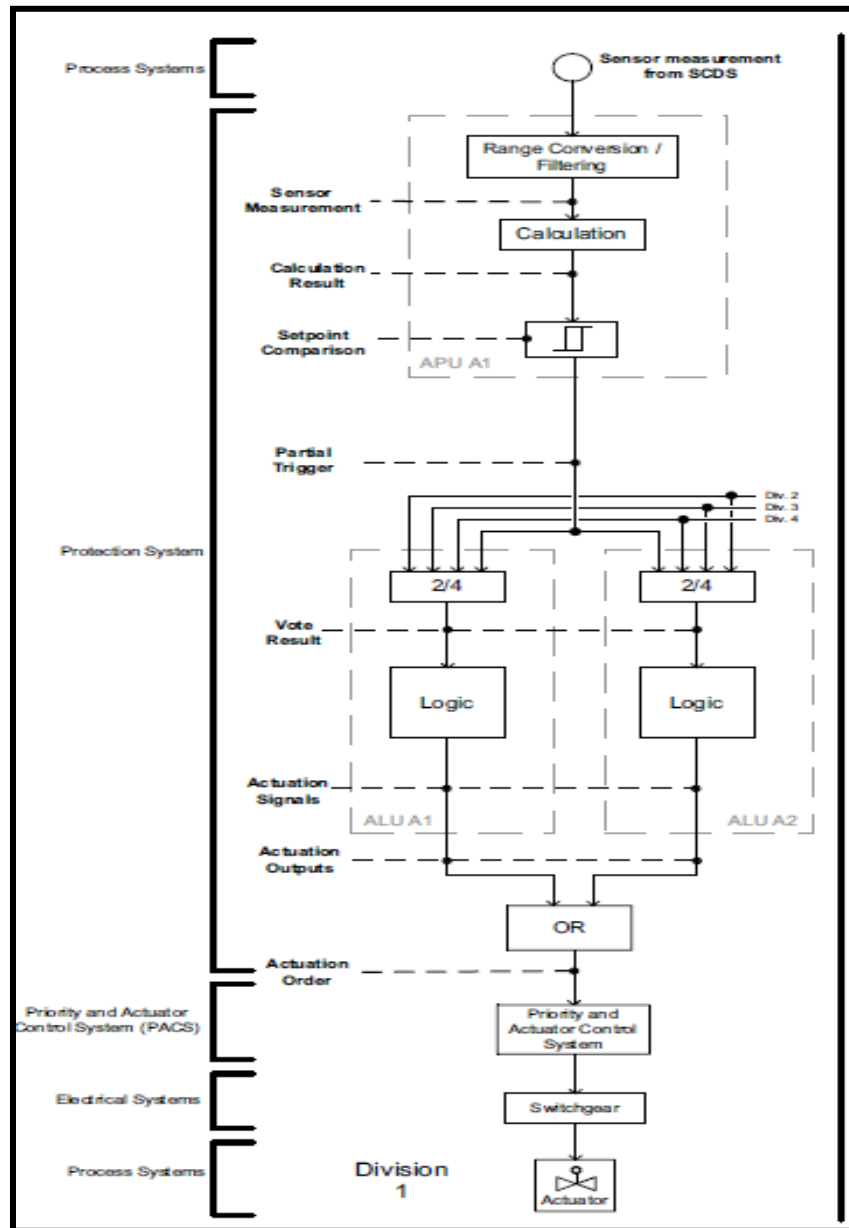
FSAR Tier 2, Figure 7.3-1, Interim Revision 3 mark-ups, provides a block diagram representation of an ESF actuation flowpath, from the sensor output to the final actuation device, for one division of the PS. The safety-related digital APU and ALU are TXS platform equipment. These TXS units consist of identical components (hardware and software) that are replicated across all PS safety division. Following the guidance of NUREG/CR-6303, for a postulated SCCF of one division's ALU(s), the failed ALU output signal could fail into a state requesting an ESF actuation. This credible failure is based on information listed in the failure modes and effect analysis results of Table A.3-1, "FMEA Results Table," located in Section A.3.2 of Technical Report ANP-10309, Revision 3. Therefore, replicating this SCCF across all PS divisions would send the faulted ALU ESF initiation signal to the PACS. The postulated CCF of the PS ALU's failed output signals to request ESF component actuation was not addressed in the D3 plant response assessment.

This particular SCCF scenario, where all PS divisions failed ALU output signals request ESF component actuation, would initiate ESF components and challenge the safety systems. However, the faulty ESF actuations would operate in the safe direction and would move to place the plant into a safe condition (i.e., SI system actuation injecting borated water into the core, closure of containment isolation valves).

In the staff's review of Technical Report ANP-10315, "U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report," Revision 0, Section 2.2.5.1.1 the staff noted that for a postulated SCCF of the ALU logic for the, ESFAS No-Go test the failed ALU logic could block the outputs of all attached PACS priority modules (see ALU output above in Figure 07.08-9). Once the "No-Go" test is initiated, the ALU logic sends a signal to block the PACS priority module outputs and also controls the release of this PACS output blocking signal. Operation of the ALU's logic to block and release the PACS priority module blocking signal is discussed in the proprietary Technical Report ANP-10315P, Revision 0, Figure 2-5. A postulated ALU SCCF that results in blocking of the PACS priority module output signals would disable the automatic PS ESF initiations, the automatic DAS ESF initiations, and the MCR operator manually initiated ESF initiations. In RAI 485, Question 07.09-69, the staff requested that the applicant demonstrate how a SCCF of the ALU logic that sends a PACS output blocking signal for the "ESFAS No-Go test" that fails to release the PACS output blocking signal, conforms to the requirements of GDC 22. In a June 22, 2011, response to RAI 485, Question 07.09-69, the applicant modified the ESFAS No-Go test so that the PACS logic will release the test blocking signal and enable requested PACS priority module's outputs after 5 seconds of the test initiation. The applicant stated that a postulated SCCF of the ALUs will not affect the release of the test's blocking signal that is now



Figure 7.8-5 Example of the PS ESF Actuation Signal Path for One Division



performed by the PACS logic. In addition, demonstration of adequate plant response of this postulated SCCF is not required since the priority module of the PACS is subject to 100 percent combinatorial testing to preclude the PACS from being considered for postulated CCFs. The applicant's response proposed to revise applicable design descriptions of the FSAR and the Technical Report ANP-10315 ESFAS No-Go test "concept" descriptions and figures. On June 13, 2011, the applicant submitted Technical Report ANP-10315 Revision 1, and the staff determined that the revised ESFAS No-Go test concept is consistent with their response and

thus, acceptable. In addition, the applicant revised FSAR Tier 2, Section 7.3.2.3.6, Interim Revision 3 mark-ups, to state:

One function of one division of the PS is tested at a time and the outputs of the PACS priority modules are disabled so that the actuators are not affected by the test. The PACS priority modules are disabled for five seconds and then they automatically exit the test mode and enable their outputs. If an ESF actuation order is generated during the time that a PACS priority module is in test mode, the outputs of the PACS priority module remain disabled until the PACS priority module exits the test mode. The ESF actuation functions are still performed using the other PS divisions.

Based on the “ESFAS No-Go Test Concept” design change, the staff finds the applicant’s June 22, 2011, response to RAI 485, Question 07.09-69 acceptable and this SCCF vulnerability has been adequately addressed. The staff considers RAI 485, Question 07.09-69 resolved with respect to D3.

#### *7.8.4.6.1 PS Subsystem Credited Signal Diversity*

The staff reviewed the I&C system for signal diversity. Technical Report ANP-10309, Revision 3, Section 1.0, last paragraph states:

The PS provides signal diversity, as described in Section 10.0, “Signal Diversity.” The signal diversity design rules presented in Section 10 represent elements of diversity described in NUREG/CR-6303 (Reference 3). AREVA NP takes credit [emphasis added] for the signal diversity within the PS, as described in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report, ANP-10304.

However, Technical Report ANP-10309, Section 10.1 states:

Signal diversity, as applied to the PS, is the use of two diverse parameters to initiate RT to mitigate the effects of the same AOO or PA. This signal diversity is not credited [emphasis added] in the diversity and defense-in-depth plant response analysis to mitigate any AOO or PA.

Furthermore, Technical Report ANP-10304, Section 4.2.4 states:

Each PS division is divided into two independent subsystems (i.e., A and B). Subsystem A in each division is redundant to Subsystem A of other divisions; the same is true of Subsystem B. The primary purpose of this arrangement is to provide [emphasis added] signal diversity for RT functions.

Finally, Technical Report ANP-10304, Section 2.2 states

Each division of the PS contains two independent subsystems to support signal diversity.

The staff was unable to determine if the applicant was crediting signal diversity between subdivisions of PS due to the apparent conflict in design descriptions. Therefore, in RAI 505, Question 07.08-45, the staff requested that the applicant clarify credit for signal diversity between PS subdivisions. **RAI 505, Question 07.08-45 is being tracked as an open item.**

The staff reviewed the design rules for PS subsystem signal diversity. Although it is now retracted and replaced by Technical Report ANP-10309, the staff's initial review noted the following description in Topical Report ANP-10281P, "U.S. EPR Digital Protection System Topical Report," Revision 0, Section 10.2, Item 7, which stated:

If a signal is required in both subsystems, it is implemented twice, once in each subsystem.

It appears to the staff that the design rules for plant sensors assigned to a PS subsystem could allow for identical signal sharing between the subsystems and this would not meet the signal diversity guidance of NUREG/CR-6303. Therefore, in RAI 413, Question 07.08-42, the staff requested that the applicant provide the actual assignments of sensor parameters and functions to the PS subsystems within a division to demonstrate how signal diversity was achieved between the PS subsystems. In a March 15, 2011, response to RAI 413, Question 07.08-42, the applicant stated that:

- Because this analysis is performed later in the detailed design process, the actual assignment of RT functions to PS sub-systems is not available at this time.
- An ITAAC commitment will be created to confirm that, for each AOO and PA, a primary and secondary RT function using different sensors as input are identified and assigned to different PS sub-systems.
- The mark-ups to FSAR Tier 1, Section 2.4, described in this response will be submitted with the response to RAI 452, Question 07.03-36.
- The design rules currently contained in Technical Report ANP-10309P, will be revised to clearly define the design rules governing allocation of functions to the PS sub-systems.

The staff agreed with the March 15, 2011, response to RAI 413, Question 07.08-42, and the proposed design modifications for PS subsystem signal diversity. However, upon the staff's review of FSAR Tier 1, Section 2.4, Interim Revision 3 mark-ups, the staff was not able to identify an ITAAC that is consistent with applicant's response to RAI 413, Question 07.08-42. Therefore, in follow-up RAI 505, Question 07.08-46, the staff requested that the applicant address the previously committed ITAAC for signal assignment among PS subdivisions.

**RAI 505, Question 07.08-46 is being tracked as an open item.** The staff's review did find that the PS subsystem rules were modified in accordance to the RAI response in Technical Report ANP-10309, Revision 3.

A PS subsystem sensor sharing rule of, "sensor inputs connected to subsystem A cannot be connected to subsystem B," would meet the most effective signal diversity attribute of NUREG/CR-6303, Section 3.2.5. As stated by the applicant in FSAR Tier 2, Revision 2, Section 19.1.4.1.1.3, "for initiating events that require reactor trip, the primary trip signal and backup trip signals are assigned to opposite subsystems." The staff finds this commitment acceptable. The diversity guidance of NUREG/CR-6303 states that related and almost coincident failures of supposedly separate systems can occur because of functional interactions, shared signals, common design errors, common environmental effects, and human actions. Signal diversity guidelines of NUREG/CR-6303, Section 3.2.5, state for all signal diversity attributes that some type of different sensing mechanism is necessary to demonstrate adequate diversity. Both PS sub-systems are able to share common functionality between them. As stated in the PS subsystem design rules of Technical Report ANP-10309, Revision 3, Section 10.2:

- If a RT function is required in both subsystems for reasons other than signal diversity, the logic is duplicated and performed in both subsystems
- If an ESFAS or permissive function is required in both subsystems, the logic is duplicated and performed in both subsystems

FSAR Tier 2, Revision 2, Section 19.1.4.1.1.3 states that for SAS, signal diversity is related to functional diversity, with one providing diverse indication and the other capturing the different functional relationships between indication and event. Functional diversity impacts the purpose, process, and performance aspects of mitigating SCCF vulnerabilities. The impact on purpose relates to differences in objectives, functional relationships, and computational interactions associated with different functions and can help address the potential SCCF vulnerabilities resulting from flawed requirements. The application of the same functionality can impact performance that can arise from having the same execution profile between systems.

It should be noted that the PS subsystems are not electrically independent and are supplied by the same instrumentation power source. As stated in Technical Report ANP-10309, Section 10.2, the cabinets of both subsystems within a division are supplied by the same divisional power sources. However, in Technical Report ANP-10304, Section 4.5, the applicant states that no credit is taken for one subsystem of the PS to function correctly, if the other fails (i.e., the PS is treated as one block). Therefore, the staff does not need to make a finding about the adequacy of the credited signal diversity between the PS subsystems for SRP BTP 7-19 conformance.

#### 7.8.4.7 *Diverse I&C System Quality Assurance*

10 CFR 50.62 states, in part, that diverse ATWS equipment must be designed to perform its function in a reliable manner. GL 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," April 1985, provides acceptable guidance for the quality assurance of diverse I&C systems and components. The four-point D3 policy of the SRM to SECY-93-087, Item 18, Position 3, states that automated backup system credited to mitigate CCFs may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions.

The staff's evaluation of the PAS quality assurance plan was discussed in Section 7.7.4.2.3 of this report. Staff found that the PAS QAP complied with the applicable quality requirements of GDC 1 and 10 CFR 50.55a(a)(1). Therefore, based on this finding, staff also concludes that the PAS addresses the quality assurance guidance of Position 3 of Item II.Q of the SRM to SECY-93-087.

FSAR Tier 2, Section 7.8.2.1.3, states that the DAS, SCDS, and PACS are provided for ATWS mitigation. The staff will evaluate the credited diverse I&C systems for conformance to the above listed requirements, policy, and guidance, in the following sections of this report.

FSAR Tier 2, Section 7.8.2.1.8, Interim Revision 3 mark-ups, state that quality requirements for ATWS equipment are implemented in accordance with GL-85-06. FSAR Tier 1, Section 2.4.24, and FSAR Tier 2, Section 7.1.1.4.7, of Interim Revision 3 mark-ups, states that the DAS design will be accomplished through a phased approach consisting of:

1. System Requirements Phase
2. System Design Phase

3. Software/Hardware Requirements Phase
4. Software/Hardware Design Phase
5. Software/Hardware Implementation Phase
6. Software/Hardware Validation Phase
7. System Integration Phase
8. System Validation Phase

FSAR Tier 2, Section 7.1.1.4.7, Interim Revision 3 mark-ups, also state that, in addition to the above listed design quality, DAS implementation will be accomplished through a phased approach consisting of:

- Criticality analysis performed for software
- Verification and validation of software is performed
- Requirements are documented in a traceable form
- DAS design is validated through acceptance test in the system validation phase

The ITAAC, listed as FSAR Tier 1, Table 2.4.24-4, Item 3.1, Interim Revision 3 mark-ups, states that a report will exist and conclude that the outputs for the DAS system requirements phase will conform to the requirements of that phase.

DAS equipment will be rated to operate under the mild environment conditions expected to exist at its location for the events that the DAS is expected to respond. In addition, the DAS is designed, fabricated, erected, and tested under the quality assurance program described in the applicant's Topical Report ANP-10266A, "AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR Topical Report," Addendum A. The staff's safety evaluation report for Topical Report ANP-10266A, Section 4.0, "Conclusion," stated:

...the AREVA QAP adequately describes the AREVA quality assurance program. Accordingly, the staff concludes that the AREVA QAP complies with the applicable NRC regulations and industry standards and can be used by AREVA for DC activities associated with the EPR."

Based on the quality assurance design descriptions stated above for the DAS, the staff concludes that the DAS quality assurance commitments addresses the ATWS quality assurance guidance of GL-85-06. Accordingly, staff finds that the DAS design meets QAP guidance of GL 85-06, Item 3.1 and the quality acceptance criteria of Item 18, Position 3 of the SRM to SECY 93-087.

FSAR Tier 2, Section 7.1.1.4.3, Interim Revision 3 mark-ups, states that the PACS is a safety-related system that is designed under the TXS quality program. The PACS does have a non-safety-related portion. However, the DAS has an electrically isolated input to the safety-related priority module and this module control the priority scheme for which actuation signal (i.e. PS, DAS, SAS, PAS) will be sent to the final component actuator. Therefore, the staff finds that the TXS safety-related quality assurance program of the PACS for the priority module

address the sufficiency of quality for credited diverse ATWS equipment required by SRM to SECY-93-087, Position 3.

There is a direct hardwired output going from the non-safety related portion of the SCDS to the DAS. Technical Report ANP-10304, Section 2.2 states that the SCDS is a safety-related system provided to condition and distribute non-safety-related sensor signals that are required in functions allocated to DAS. The SCDS is segmented within each division to include safety-related and non-safety-related equipment for the conditioning and distribution of safety-related and non-safety-related instrumentation, respectively. FSAR Tier 2, Section 7.1.1.4.8, Interim Revision 3 mark-ups, states that the SCDS is classified as safety-related and that the SCDS is designed under the TXS quality program. The staff reviewed FSAR Tier 1, Section 2.4.25; FSAR Tier 2, Sections 7.1 and 7.8; as well as Technical Report ANP-10304, and was not able to locate applicable QA design descriptions for the non-safety portion of SCDS. In addition, the staff reviewed FSAR Tier 1, Table 2.4.25-3, and determined that the table only addresses safety-related SCDS outputs and did not list any DAS connections for the SCDS safety-related system outputs. Similarly, the staff could not identify quality assurance commitments regarding the non-safety-related portions of SICS that are used in conjunction with DAS. Therefore, in RAI 505, Question 07.08-48, the staff requested that the applicant address the quality assurance for the non-safety portion of SCDS and SICS. **RAI 505, Question 07.08-48 is being tracked as an open item.**

#### *7.8.4.8 DAS Surveillance and Testing*

The guidance of SRP Section 7.8 states that the applicant/licensee should identify the test, maintenance, surveillance, and calibration procedures. These provisions should be consistent with the guidance of GL 85-06 and its enclosure. The ATWS mitigation system should be testable at power (up to, but not necessarily including, the final actuation device).

FSAR Tier 2, Section 7.8.1.1.3, Interim Revision 3 mark-ups, state that the DAS will be periodically tested. It also states that DAS system operation status (i.e., bypass, initiate, standby, normal), power availability, and any system faults or messages pertinent to plant operation will be sent to both PICS and SICS for display to the operators in the MCR. Sensors that are shared by PS and DAS are periodically tested as part of the PS surveillance. GL-85-06, Section XI provides guidance for the capability to test the DAS at power. While there is a commitment to periodically test the DAS, the staff did not find sufficient design description as to the capability to test the DAS at power. Therefore, in RAI 505, Question 07.08-47, the staff requested that the applicant clarify the capability to test DAS at power. **RAI 505, Question 07.08-47 is being tracked as an open item.**

Upon closure of RAI 505, Question 07.08-47, the will conclude that the applicant identified applicable surveillance and test criteria in accordance with GL-85-06 and that these criteria are consistent with the quality guidance of GL-85-06. The staff finds that the applicant has provided sufficient design descriptions and design commitments for DAS quality assurance, equipment qualification, maintenance and surveillance and, therefore, the staff finds that DAS QA design commitments address the sufficiency of quality for credited diverse back-up systems as stated by Item 18, Point 3 of the SRM to SECY-93-087 and required by 10 CFR 50.62..

## DAS and PAS Equipment Reliability

SRP Section 7.8 guidance states that diverse I&C systems design should limit the potential for inadvertent actuation and challenges to safety systems and that the DAS/ATWS mitigation logic should be designed such that, once initiated, the mitigation function will go to completion.

FSAR Tier 2, Section 7.8.1.1.3, states that the DAS voting logic is such that single failures do not result in spurious actuations of the automatic DAS functions. FSAR Tier 2, Section 7.1.1.4.7, Interim Revision 3 mark-ups, state that the DAS acquires plant process sensor output signals from the SCDS and compares the outputs to associated monitored plant parameter setpoint thresholds at each DAS's diverse actuation unit (DAU). Hardwired connections are provided between each DAS division's DAU to share any DAU's trip actuation request and two-out-of-four voting is done in each DAU. FSAR Tier 2, Figure 7.1-13, displays the DAS architecture and design operation. The DAS functions are designed so that once initiated, they proceed to completion. Accordingly, based on the DAS equipment design operation reliability and staff approved QA design for the DAS, the staff finds that the DAS addresses the SRP Section 7.8 guidance for potential for inadvertent actuation and completion of protective action.

### **7.8.5 Combined License Information Items**

No applicable items were identified in the FSAR. No additional COL information items need to be included in FSAR Tier 2, Table 1.8 2, "U.S. EPR Combined License Information Items," for reactor trip system consideration.

### **7.8.6 Findings and Conclusions**

Based on the review described in this section, and upon satisfactory closure of RAI 505, Questions 07-08-43 through 07-08-49 and RAI 512 Question 07-08-50, which are being tracked as open items, the staff will be able to find that the applicant meets the requirements of 10 CFR 50.55a(h), 10 CFR 50.62, and GDC 1, GDC 13, GDC 19, GDC 22, and GDC 24 once the open items in this section have been satisfactorily addressed. Specifically, the staff should be able to find that the applicant addressed the applicable requirements as described in the following paragraphs.

Based on the credited diverse system's QA commitment to the quality assurance guidance of GL 85-06, the staff finds that the applicable quality assurance requirements of GDC 1 have been met.

Based on the applicant's diverse, independent, and direct hardwired signal paths from the system components to SICs, which bypass the software-based PS, the staff finds that postulated failures of the diverse monitoring or display systems will not influence the functioning of the reactor trip system or ESF system actuations and will not induce operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation. Accordingly, the staff finds that the diverse I&C design addresses the acceptance criteria of BTP 7-19, Section B.3, Item 5. In addition, based on the staff's evaluation of the U.S. EPR diverse manual displays and controls, located in Section 7.8.4.1.2 of this report, the staff concludes that these controls and displays are independent and diverse from the safety computer system, and are sufficient for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. Therefore, the staff

concludes that the manual controls and displays fulfill the guidance of the SRM to SECY-93-087, Item 11Q, Position 4.

Based on the design commitment to develop and implement electrical isolation in accordance to the guidance of RG 1.75 and SRP BTP 7-11, the use of these qualified isolation devices on all PS to credited diverse non-safety-related I&C systems connections, and the use of separate and independent power supply sources used between the PS and the credited non-safety-related diverse I&C systems, and the physical separation between safety-related and non-safety-related diverse I&C equipment, the staff concludes that the independence of these systems from safety systems complies with the requirements of GDC 24.

Technical Report ANP-10304 adequately demonstrates diverse plant system mitigation response to a PS postulated CCF concurrent with an AOO or PA. Specifically, the plant response analyses did not result in radiation release exceeding 10 percent of the 10 CFR Part 100 guideline for AOOs and did not result in radiation release exceeding the 10 CFR 100 guideline values for PAs. Therefore, the staff finds that the D3 assessment adequately addressed the 12-step diversity analysis of NUREG/CR-6303. The staff finds that the D3 plant response contained in Technical Report ANP-10304 meets the D3 SCCF acceptance criteria of BTP 7-19, Section B.3, Items 1 and 2. Based on the staff's evaluation of the D3 design plant response, functions and design, the staff concludes that the D3 diverse systems functional requirements, independence requirements, and design commitments fulfill Points 1, 2, and 3 of the SRM on SECY-93-087, Item II.Q. Accordingly, the staff finds the applicant's D3 I&C design implement's component and functional diversity to prevent loss of the protective function for postulated SCCF of the PS concurrent with an AOO or PAs, and thus, complies with the requirements of GDC 22 and IEEE Std 603-1998, Clause 5.16.

Based on the review of D3 diverse I&C system status information and manual initiation, the staff concludes that information is provided to monitor the system over the anticipated ranges for normal operation, AOOs, and PAs to address the NRC's four point D3 policy as stated in SRM to SECY 93-087, Item II.Q. These manual controls were found by staff to be independent of the safety-related PS. The staff also found that the diverse I&C systems appropriately support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Accordingly, the staff finds that the design of the diverse I&C systems complies with the requirements of GDC 13 and GDC 19.

Based on the staff's evaluation of the U.S. EPR-credited ATWS mitigation systems, the DAS, PAS, the non-safety-related portions of the SICS, the non-safety-related portions of the SCDS, and PACS, the staff finds that these ATWS mitigation systems comply with the specific requirements of 10 CFR 50.62.

## **7.9 Data Communication Systems**

### **7.9.1 Introduction**

The digital I&C systems utilize data communication systems as an integral part of the overall I&C architecture. Data communication systems used in the I&C design are primarily described in FSAR Tier 2, Section 7.1; Technical Report ANP-10309, "U.S. EPR Protection System Technical Report," Revision 3; and Topical Report EMF-2110(NP)(A), "TELEPERM TM XS: A Digital Reactor Protection System," Revision 1. The following sections describe the staff's review of the U.S. EPR data communication systems.



## 7.9.2 Summary of Application

**FSAR Tier 1:** The FSAR Tier 1 information associated with this section is found in FSAR Tier 1, Section 2.4.

**FSAR Tier 2:** The applicant has provided a system description in FSAR Tier 2, Section 7.1, which is summarized as the following.

The primary I&C systems used for control and monitoring in the plant are collectively referred to as the distributed control system. The DCS performs the majority of signal input processing, automation, operator interface, annunciation of abnormal conditions, and actuator output functions in the plant. FSAR Tier 2, Section 7.1, describes the data communication process between different I&C systems within the DCS. This includes communication within the safety I&C systems, communication between safety I&C systems and non-safety systems, and communication between various non-safety plant control systems.

Data communication within safety I&C systems are based on the TXS communication process. As described in this Topical Report EMF-2110, a separate communications module is used to process communication between function processors. All communications between safety function processors are cyclic and performed with the following process. An output message is transmitted into the Dual-Port Random Access Memory (DPRAM) of the interface to the communication module. The message is prepared by attaching the appropriate header information such as message number, Cyclic Redundancy Check (CRC), and address. The data contained within each type of message varies according to the type of message, but is fixed for each type. The data is sent serially via the network medium in accordance with the protocol used in the interface module of the destination system. A message is then received in the communication module input buffer, and is checked for proper sequence, format, and CRC. The message is then sent to the DPRAM at the interface between the communication processor and the function processor, and the function processor then reads the input message from the DPRAM.

The TXS platform uses both the SINEC L2 Process Fieldbus (Profibus) and SINEC H1 Ethernet communication protocols. FSAR Tier 2, Section 7.1.1.2.3 states that the U.S. EPR only uses the TXS Profibus communication protocol for safety-related communication. Data communication between different safety I&C function computers are achieved either through point-to-point bi-directional and uni-directional links or through bi-directional ring networks. Communication between safety function computers can be intradivisional or interdivisional.

Data communications from the safety I&C systems to non-safety plant control systems through the Monitoring and Service Interface and a gateway are achieved through uni-directional data links. This includes communication from SAS and PS to various non-safety I&C systems via the non-safety-related automation bus. In addition, the SAS, PS, and RPMS also communicate bi-directionally with the non-safety-related Service Unit through the MSI for monitoring, diagnostic, parameters changes, and software modification purposes on a temporary basis. The communication path between the SU and the divisional MSIs for PS and SAS is isolated while not in use by hardwired disconnects using a key-operated isolation switch. This isolation switch also prevents connection of the SU to more than a single division at a time. The gateways perform communication protocol translation between the TXS protocol used for safety I&C systems and the protocol used for the automation bus.

Data communication between non-safety control systems, such as PICS, RCSL, TG I&C, and PAS use the automation bus. The automation bus also interfaces with a HMI bus within the PICS system. In addition, as specified in FSAR Tier 2, Section 10.2.2.5, two redundant communications paths for each turbine-generator package from the TG control system main control cabinet to the operator workstation are provided. In addition, two redundant communications paths within the TG I&C system are provided to connect to the plant PAS.

In addition to data communication for safety and non-safety systems, hardwired connections are also used within and between safety I&C systems and non-safety I&C systems. This includes hardwired connections between the proposed SCDS with safety and non-safety I&C systems, as described in FSAR Tier 2, Interim Revision 3 mark-ups, in a June 22, 2011, response to RAI 442, Question 07.01-26. The functions of the SCDS are to receive input signals from dedicated I&C systems and provide conditioned, standard analog output signals to multiple DCS subsystems.

**ITAAC:** The ITAAC associated with data communication systems are given in FSAR Tier 1, Table 2.4.1-7, "Protection System ITAAC," Table 2.4.4-6, "Safety Automation System ITAAC," Table 2.4.5-3, "Priority and Actuator Control System ITAAC," and Table 2.4.26-4, "Rod Position Measurement System ITAAC."

**Technical Specifications:** There are no Technical Specifications associated with data communication systems.

### **7.9.3 Regulatory Basis**

The relevant requirements of NRC regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, Section 7.1, Section 7.9, and Appendix 7.1-A and are summarized below. Review interfaces with other SRP Sections also can be found in NUREG-0800, Section 7.1.

Requirements applicable to data communication systems are as follows:

1. GDC 24, "Separation of Protection and Control Systems"
2. 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the January 30, 1995, correction sheet. The minimum requirements that are applicable to all DCSs are IEEE Std 603-1991, Clause 5.6.3, "Independence Between Safety Systems and Other Systems"
3. 10 CFR Part 50, Appendix A, GDC 1, "Quality Standards and Records"
4. 10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety"

Acceptance criteria adequate to meet the above requirements include SRP Table 7-1, Section 3 (Staff Requirements Memoranda), Section 4 (Regulatory Guides), and Section 5 (Branch Technical Positions), which list the SRP acceptance criteria applicable to data communication systems important to safety.

#### 7.9.4 Technical Evaluation

Objectives of the staff's review of the FSAR Tier 2, Section 7.1 are to confirm that the data communications systems design satisfies NRC regulations through a set of acceptance criteria, and that it can perform its safety functions for all plant conditions. NUREG-0800, Section 7.9, "Data Communications Systems," lists the following major design considerations that should be emphasized for the review of data communications systems:

- quality of components and modules
- data communications systems software quality
- performance
- reliability
- time coherency of data
- control of access
- single failure criterion
- independence
- system testing and inoperable surveillance
- protocols
- EMI/RFI susceptibility
- diversity and defense-in-depth
- data communications systems exposed to seismic hazard

The staff also identified, "Control System Data Communication Functions," as another area of review for data communication systems. The staff's review of, "Time Coherency of Data," and, "Protocols," has been combined with the review of, "Reliability" in Section 7.9.4.2 of this report. Several of these design considerations are fully or partially addressed in other sections of this report, as indicated in Table 7.9-1 below.

**Table 7.9-1 Section 7.9 Design Considerations Referenced in Other Sections of this Report.**

<b>Design Considerations</b>	<b>SER Section(s)</b>
Quality of Components and Modules	7.1.4.3 and 7.1.4.7
Data Communications Systems Software Quality	7.1.4.3 and 7.1.4.7
Single Failure Criterion	7.1.4.5
System Testing and Inoperable Surveillance	7.1.4.13, and 7.5.4.1

<b>Design Considerations</b>	<b>SER Section(s)</b>
EMI/RFI Susceptibility	7.1.4.8
Diversity and Defense-in-Depth	7.8
Data Communication Systems Exposed to Seismic Hazard	7.1.4.8
Physical Separation and Electrical Isolation	7.1.4.10

#### 7.9.4.1 *Performance*

10 CFR 50.55a(a)(3) allows an applicant under 10 CFR Part 52, to propose alternatives to the requirements of 10 CFR 50.55a(h). The U.S. EPR design certification applicant proposes to use IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as an alternative to 10 CFR 50.55a(h), which requires the use of IEEE Std 603-1991. Section 7.1.4.1 of this report discusses the staff's evaluation and approval of this alternative. IEEE Std 603-1998, Clause 5.5 requires safety systems be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. In addition, IEEE Std 603-1998, Clause 4.j requires, as a part of the design basis, identification of the critical points in time or the plant conditions, after the onset of a design basis event.

To meet IEEE Std 603-1998, Clause 5.5 and Clause 4.j, data communication systems in support of the protection system should demonstrate real-time performance in accordance with SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance." SRP BTP 7-21 stipulates that:

1. The level of detail in the architectural description should be sufficient that the staff can determine the number of message delays and computational delays interposed between the sensor and the actuator
2. Data rates and data bandwidths should be reviewed including impact by environmental extremes
3. Sufficient excess capacity margins should be available to accommodate future increase

In addition, limiting response times should be consistent with safety requirements. Digital computer timing should be consistent with the limiting response times and characteristics of the computer hardware, software, and data communication systems.

FSAR Tier 2, Section 7.1.2.5.16 states that applicable I&C systems listed in FSAR Tier 2, Table 7.1-2 are designed to meet the guidance of SRP BTP 7-21. The design features that provide for real-time, deterministic behavior of the SICS, PS, and SAS are described in Topical Report EMF-2110(NP)(A). Topical Report EMF-2110(NP)(A), Section 3.1.1.5 describes the TXS design requirements for deterministic system behavior with guaranteed maximum computing and reaction times and constant communication loads. This section states that the design requires each process unit to process its assigned function in a strictly cyclical manner with a predefined cycle time. During each operating cycle, the sequence of processing steps is always the same. The control flow is independent from the process data. The message sizes and communication rates are constant, resulting in constant communication loads under all

circumstances. In addition, the communication protocols used in the TXS system do not require acknowledgement of the transmitted message by the receiver. Thus, the processor receiving the message cannot influence the operation of the sending processor. The staff finds the deterministic behavior of the TXS system, as described in Topical Report EMF-2110(NP)(A), Section 3.1.1.5 ensures adequate performance of the data communication system to accomplish its safety function to meet IEEE Std 603-1998, Clause 5.5.

In the safety evaluation report for Topical Report EMF-2110(NP)(A), Section 4.3, the staff stated that the TXS system architecture and the system response time test methodology as discussed in the topical report demonstrated that the TXS system design is consistent with SRP BTP HICB-21. SRP BTP 7-21 provides updated guidance to SRP BTP HICB-21, Revision 4. Based on the staff's conclusions in the safety evaluation report for Topical Report EMF-2110(NP)(A), the staff finds the response time test methodology is acceptable. However, the staff included plant-specific action item (PSAI) 11 in the safety evaluation report for licensees who reference this topical report to perform protection system response time tests in accordance with plant technical specification requirements. PSAI 11 required licensees to evaluate plant-specific accident analysis to confirm that a TXS reactor trip system includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown (safety analysis confirmation for accuracy and time response) consistent with accident analysis presented in Chapter 15 of the plant safety analysis report. To address this PSAI, in RAI 1, Question 4, the staff requested that the applicant clarify how the guidance of SRP BTP 7-21 is addressed in the design of the PS to meet IEEE Std 603-1998, Clause 4.j. This request was documented in RAI 1 of Topical Report ANP-10281P, "U.S. EPR Digital Protection System Topical Report."

The applicant submitted Topical Report ANP-10281 to describe the digital PS within U.S. EPR design. The staff reviewed this topical report and had several RAI exchanges with the applicant. In letter, "Withdrawal of ANP-10281P, U.S. Digital Protection System Topical Report," (ADAMS Accession Number ML092520146) the applicant withdrew Topical Report ANP-10281. On July 1, 2011, the applicant submitted Technical Report ANP-10309, "U.S. EPR Protection System Technical Report," Revision 3

In an August 21, 2007, response to RAI 1, Question 4 for Topical Report ANP-10281P, the applicant stated that the methodology used to estimate the response time of the computerized portion of the PS establishes a theoretical bounding response time for the typical types of functions performed by the PS. This response states that the total response time for a given function consists of several sub-intervals that span from a process variable exceeding a pre-defined limit to completion of the protective function. The sub-interval addressed herein accounts for the computerized portion of the protection channel, and is defined as the time from sensor conditioning output to RT breaker input terminals for RT functions, or to input terminals of the PACS for ESF actuation functions. The final response time of the PS will be verified to be within the bounding time limits established for the PS.

The applicant provided an analysis of the allocation of time delays to the computerized portion of the PS in Attachment B of a December 3, 2007, response to "Second Request for Additional Information for the U.S. Digital Protection Topical Report." In addition, FSAR Tier 2, Table 15.0-7, "Reactor Trip Setpoints and Delays Used in the Accident Analysis," and Table 15.0-8, "Engineered Safety Features Functions Used in the Accident Analysis," list the time delay assumed for each protective function performed by the PS. The applicant verified that the estimated response times provided in Attachment B of their response to, "Second Request for Additional Information for the U.S. Digital Protection Topical Report," were

consistent with the time delays assumed in FSAR Tier 2, Tables 15.0-7 and 15.0-8, as documented in a November 13, 2009, response to RAI 286, Question 07.09-47. In this RAI, the staff requested that the applicant identify the ITAAC item that verifies the as-installed PS response time, from sensor output to final actuation device, is bounded by the PS response time used in FSAR Tier 2, Tables 15.0-7 and 15.0-8 accident analysis. The staff also requested that the applicant describe how the time delay of the PACS module is incorporated into the PS response time analysis provided in the 12/3/2007 response to RAI 1, Question 4, in Attachment B addressing review of Topical Report ANP-10281P.

In a November 13, 2009, response to RAI 286, Question 07.09-47, the applicant stated that the bounding PS response times discussed in the, "Second Request for Additional Information for the U.S. Digital Protection Topical Report," Attachment B are consistent with the response time assumptions used in the accident analysis and listed in FSAR Tier 2, Tables 15.0-7 and 15.0-8. The applicant also included this analysis as part of Technical Report ANP-10309P, Revision 3, Appendix B. In a February 26, 2010, response to RAI 285, Question 07.03-25, the applicant addressed verification that the PS response times support accident analysis assumptions. The PACS is not included in the PS response time analysis. Time delays introduced by the priority module in the PACS are included with the response time of the actuator it controls and is verified through response time testing of the actuator. The staff finds the applicant's February 26, 2010, response to RAI 285, Question 07.03-25, acceptable to ensure consistency of the PS response time analysis and the response time assumptions used in the accident analysis. However, the staff finds that the applicant's response did not demonstrate how the time delays introduced by PACS have been incorporated in the response time testing ITAAC (i.e., Protection System ITAAC, Table 2.4.1-7, Item 4.24). The staff determined time delays introduced by the PACS should be tested to verify that the PACS is bounded by the Chapter 15 limit, and that the applicant should clarify the Chapter 15 definition of "I&C delay," as described in RAI 414, Question 07.03-30. In an August 19, 2011, response to RAI 414, Question 07.03-30, the applicant stated that the response time testing of the PS in the PS ITAAC and surveillance testing is the testing of the time delay as defined in FSAR Tier 2, Tables 15.0-7 and Table 15.0-8. This time delay includes I&C delay. The I&C delay time listed includes PS equipment response time and PACS equipment response time. The applicant states that the term "I&C delay" in FSAR Tier 2, Table 15.0-7, Note 2, and FSAR Tier 2, Table 15.0-8, Note 4 will be clarified to include the PS computerized portion and PACS delay. The staff finds the response acceptable to demonstrate that the PACS is included in the overall response time testing. Specifically, the staff finds that the term, "I&C delay," in FSAR, Tier 2, Table 15.0-8, Note 4 will be clarified to include the PS computerized portion and PACS delay is acceptable to include PACS delay in the overall I&C system response time limits. Based on the response time analysis provided in Technical Report ANP-10309P, Revision 3, Appendix B the proposed modifications to clarify the term, "I&C delay," to include PACS delay, and the response time testing and analysis ITAAC in Protection System ITAAC, Table 2.4.1-7, Item 4.24, the staff finds that the PS data communication is sufficient to address the requirements of IEEE Std 603-1998, Clause 4.j. Specifically, the staff finds that the delays introduced by the data communication system in the PS will be verified through the response time analysis and testing to confirm that the Chapter 15 response time limits are met.

#### 7.9.4.2 *Reliability*

##### 7.9.4.2.1 *Data Communication Systems Reliability*

IEEE Std 603-1998, Clause 5.15 requires appropriate analysis be performed on the system design for which either quantitative or qualitative reliability goals have been established to

determine that such goals have been achieved. To meet the requirements of IEEE Std 603-1998, Clause 5.15, data communication systems in support of safety functions should demonstrate sufficient reliability in accordance with the acceptance criteria described in SRP Section 7.9. SRP Section 7.9 states that the data communication system design should identify and address potential hazards. The design should preclude the inadvertent activation of unneeded data communication functions that is included in the data communications system design. Error detection should be at least as good as a four-byte CRC. Corrupted messages (missing or corrupted packets), missing messages, and duplicate messages should be detected and repaired. SRP Section 7.9 also states that methods should be employed to ensure the correct sequence of data packets at receiving data communication systems nodes. In addition, protocols proposed for use, whether standard or proprietary, should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

FSAR Tier 2, Section 7.1.2.6.26 states that safety systems are designed to accomplish their safety functions in a reliable manner to support overall plant availability. The software used for data communication systems in support of safety functions within the U.S. EPR digital I&C safety system design follows the same high quality software development process detailed in Topical Report ANP-10272, "Software Program Manual for TELEPERMTM XS Safety Systems," Revision 3. The review of unneeded data communication functions and its impact on the supported safety function, as well as the software hazards analysis on the data communications software, were completed as part of the review for the Topical Report ANP-10272. The safety evaluation report for Topical Report ANP-10272P documents the staff's review of this topical report. In addition, a summary of this review is described in Section 7.1.4.7 of this report.

In the safety evaluation for Topical Report EMF-2110(NP)(A), Section 2.2.1.1, the staff described the data communication functions within the TXS operating software. This section states the TXS runtime environment controls all processing cycle activities, including communication. The TXS processing cycle is started by the central control unit of the RTE by triggering the internal MicroNet controller to transfer the messages in the receiving DPRAMs of all linked communication modules into the corresponding message input buffers. After the integrity of the message is checked by means of a 16-bit CRC, for the occurrence of random bit errors, and by means of a sequence increment (to ensure that a new message has been received), the message is flagged as a valid or an invalid message for subsequent processing. The Run Time Engine software automatically marks the invalid message and all signals stored in this message with the ERROR status flag. Signals marked with ERROR status flag are excluded from further processing by the function blocks. During function diagram processing, the valid signals are further processed to determine out-of range conditions and defective-instrument conditions. All provisional signals are stored in dedicated signal buffers during function diagram processing. After function diagram processing has been completed, the central control unit triggers the function diagram group output function to create output message data from the results of the function group processing. The Run Time Engine then adds a message header to the message data, which includes a CRC checksum and the cycle counter, and stores the output message data in the message output buffers. As the last step in the processing cycle, the Run Time Engine triggers the communication control program (MicroNet) to transfer the message data from the output buffers into the sending DPRAMs of the respective communication processor. This message data is then sent to other subracks and the MSI.

In addition to validating the communication messages, the Run Time Engine also increments a local cycle counter to support error detection. This 16-bit counter forms the internal relative short-time base sign-of-life clock for communication and for time-sequencing fault signals. The cycle count of the Run Time Engine at the time of transmission is appended to every message.

This information is used by the receiving processor to monitor the validity of the message and the correct functioning of the transmitter.

Topical Report EMF-2110(NP)(A), Section 2.9 describes the use of data message sequence counters to ensure that the received message is in correct sequence, and that incorrect or old messages are marked invalid. In addition, Topical Report EMF-2110(NP)(A), Figure 2-19, "Process Cycle," depicts the steps within the TXS operating system processing cycle where the message sequence is checked for correctness, and where the next message sequence counter is incremented. Topical Report EMF-2110(NP)(A) states that two communication protocols are used in the TXS. Data communication to the plant process information system and other non-safety information systems and to the SU use the SINEC H1 protocol, which operates over Ethernet (TXS Ethernet protocol.) Communication between different processors within the TXS safety system is over fiber optic connections using the SINEC L2 Profibus protocol. Profibus is a fieldbus using asynchronous character transmission. It uses a modified master-slave arrangement, with masters exchanging the right to control the bus by passing a token. The H1 protocol is a Siemens proprietary Ethernet fieldbus protocol. Communication between different processors is done by messages. These messages can contain signals from Function Diagram Group (FDG) modules (data messages); control -commands from the SU (control messages); or error messages, trace data, or command responses to the SU (signaling messages). Topical Report EMF-2110 also states that the SINEC L2 communication control works autonomously without any possibility to influence the strictly cyclic processing of the linked processor systems.

Although the TXS operating system does not support the 4-byte CRC error detection stipulated in SRP Section 7.9, the staff finds the use of the 16-bit CRC for error detection in conjunction with the other error detection methods (e.g., message header checks, message sequence checks, and local cycle counter) demonstrate that the U.S. EPR safety systems data communication system adequately meets the reliability requirements of IEEE Std 603-1998, Clause 5.15. In addition, based on the information presented in Topical Report EMF-2110(NP)(A), the staff finds the TXS system adequately ensures that out of sequence messages are flagged during every processing cycle to meet the requirements of IEEE Std 603-1998, Clause 5.15.

The staff evaluated the usage of the SINEC L2 Profibus protocol for communication between different safety processors, and the usage of H1 protocol for communication from safety processors to plant process information systems and to the SU, and found that the applicant did not demonstrate how these protocols communicate deterministically for safety applications. Specifically, the applicant did not provide an analysis of hazards and performance of these two protocols to demonstrate that data communication using these protocols is deterministic. This is of special concern for SINEC H1 protocol since it is Ethernet-based, which typically has been shown to be non-deterministic. Therefore, in RAI 442, Question 07.09-61, the staff requested that the applicant provide additional information to demonstrate how data communication, using these protocols are deterministic. In a March 2, 2011, response to RAI 442, Question 07.09-61, the applicant proposed to include in FSAR Tier 2, Section 7.1.1.6.4 a discussion on the use of cyclic processing in I&C safety systems, which provides for deterministic communication. Specifically, the safety-related I&C systems use proprietary, time-triggered operating systems that do not rely on hardware and interrupt only on cyclic processing of the software. Since there are no process-driven interrupts, every operation is cyclic and predictive, which verifies that the output of messages on networks link prevents collision. The hardware components only read the incoming memory buffer or generate a packet to send only when the operating system generates the order. In addition, the communication process sends information written in memory and writes in memory received information. Packet numbering



verification shows that a packet is only processed once without synchronizing both tasks. As stated above, FSAR Tier 2, Section 7.1.1.2.3 as part of a June 22, 2011, response to RAI 442, Question 07.01-26, the applicant stated that for the U.S. EPR, only the TXS Profibus communication protocol is used for safety related communication. Furthermore, based on a June 22, 2011, response to RAI 442, Question 07.01-31, the applicant modified the QDS to be non-safety-related. Data communication between the QDS and PS is uni-directional from the PS to the QDS. The isolation of the QDS from the PS is provided by the PS. The evaluation of the isolation between the PS and QDS is documented in Section 7.9.4.5 of this report. The data communication link between the PS and the QDS is classified as non-safety-related and, therefore, does not need to meet the requirements of IEEE Std 603-1998, Clause 5.15. Based on the information provided, the staff finds that the I&C safety systems design is adequate to provide for data communication reliability to meet IEEE Std 603-1998, Clause 5.15. Specifically, the staff finds the use of cyclic processing without the use of process driven interrupts and the use of the Profibus protocol for all safety applications enable deterministic data communication for U.S. EPR I&C safety systems.

#### *7.9.4.2.2 Effects of Data Storms*

10 CFR Part 50, Appendix A, GDC 13 requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

FSAR Tier 2, Section 7.1 describes the interconnections of non-safety I&C systems via the HMI bus and automation bus. The HMI bus and automation bus are non-safety-related buses that interconnect I&C safety systems with the PICS as shown in Figure 7.9-1 of this report. The automation bus also allows various non-safety-related control systems, such as the RCSL, the PICS, and the TG I&C to communicate with each other. If the technology of the automation bus and HMI bus for which the applicant selects is Ethernet-based, the applicant should address the potential for data storms in order to provide reliable data transmissions on these buses to support control system functions required by GDC 13. The original application did not address the design of the automation bus and HMI bus to preclude the susceptibility of this network to data storms. In RAI 286, Question 07.09-49, the staff requested that the applicant clarify how the effects of data storms are addressed for the automation and HMI buses. In a March 5, 2010, response to RAI 286, Question 07.09-49, the applicant stated that sound engineering and design practices will be applied to development of the PICS automation bus, HMI bus, and the DCS systems connected to the bus. PICS automation and HMI buses will be designed to withstand data traffic, and the interfacing DCS systems will be designed with thresholds for network traffic that are consistent with maximum data rates of the buses. Specific design details regarding preclusion of data storm events on a non-safety-related network depends on the specific technology chosen for these non-safety-related networks, and they are not included in the FSAR. PICS will have adequate bandwidth needed to reliably operate the process systems in the reactor plant and to keep the plant reliably online. The staff finds the commitment to provide design features to preclude data storm events for the non-safety networks, in addition to the safety system design features that prevent data storms from affecting safety functions (e.g., cyclic processing, separate communication and function processors, etc.) are adequate to ensure reliability of safety functions. In follow-up RAI 442, Question 07.09-62, the staff requested that the applicant include the March 5, 2010, response to RAI 286,

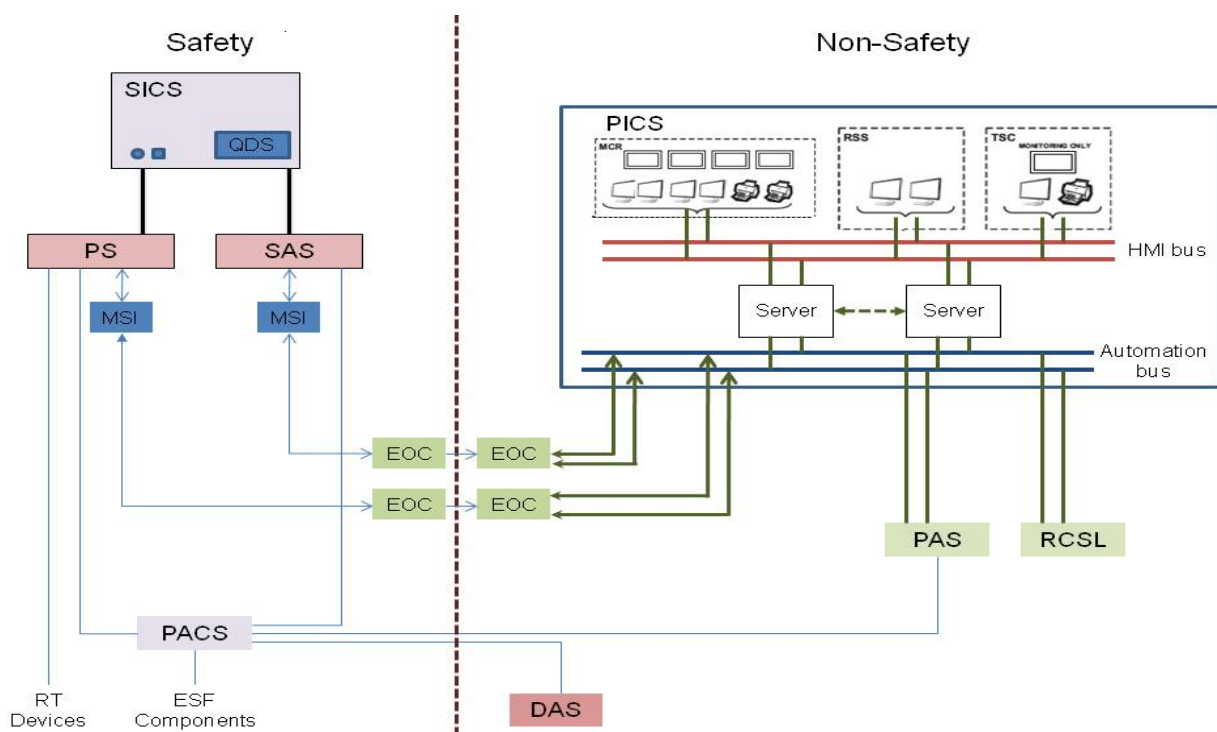
Question 07.09-49 into FSAR Tier 2. In a February 18, 2011, response to RAI 442, Question 07.09-62, the applicant committed to revise FSAR Tier 2, Section 7.1.1.3.2, to include the description of design commitments to preclude data storms. Based on their commitment to include design criteria in FSAR Tier 2, Section 7.1.1.3.2 to withstand data traffic and the interfacing DCS systems will be designed with thresholds for network traffic that are consistent with maximum data rates of the buses, the staff finds that the applicant has addressed the effects of data storms to demonstrate that the automation and HMI buses will be sufficiently reliable as required by GDC 13.

#### 7.9.4.3 *Control of Access*

IEEE Std 603-1998, Clause 5.9, requires the safety system design to permit the administrative control of access to safety system equipment. To meet the requirements of IEEE Std 603-1998, Clause 5.9, data communication systems in support of safety functions should demonstrate that adequate access controls are incorporated into the design of the data communications system in accordance with the acceptance criteria described in SRP Section 7.9. SRP Section 7.9 states that data communication should not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators. Remote access to safety systems should not be implemented. In addition, RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Revision 2, Regulatory Positions C.2.1-2.9 provide additional criteria for access control.

FSAR Tier 2, Section 7.1.2.6.20 discusses how U.S. EPR safety systems meets requirements of IEEE Std 603-1998, Clause 5.9. The applicant provided FSAR Tier 2, Section 7.1, Interim Revision 3 mark-ups, to address the design changes to the U.S. EPR I&C systems architecture. These mark-ups were submitted as part of a June 22, 2011, response to RAI 442, Question 07.1-26. FSAR Tier 2, Section 7.1.2.6.20, Interim Revision 3 mark-ups states that access to the cabinets of the SICS, PS, SAS, SCDS, and PACS are provided via doors that are normally closed and locked. Door positions are monitored, allowing operators the ability to investigate unexpected opening of cabinet doors. Cabinets are also located in physically separate equipment rooms within the four Safeguard Buildings and can only be accessed by authorized personnel. The SICS equipment is located in the MCR and RSS. Both areas are controlled security areas. The FSAR mark-ups also include modifications to FSAR Tier 2, Section 7.1.1.6.4 to provide a description of an additional hardwired disconnect between the SU and the divisional MSIs for the PS and SAS. The hardwired disconnect isolates the PS and SAS from the SU until a temporary connection is established between the SU and the divisional MSI of the PS or SAS. This is achieved with a key-operated isolation switch located in the MCR. This allows the main control room operators to monitor the position of the isolation switches. A local connection point for SU connection is located in the lockable MSI cabinet in each PS and SAS division. Control room annunciation will communicate the access to the local connection using the door open alarm. This local connection is isolated by a key-operated isolation switch. The isolation switches are keyed so that a single key operates the eight switches (four MCR and four local), and they are physically retained in the switch when positioned to allow the SU connection to the system to prevent connection of a SU to more than a single division. This switch is hardwired and physically prevents the connection of a SU to more than a single division of the PS or SAS at a time. The keys associated with the CPU state switches and the isolation switches are part of the key control program. FSAR Tier 2, Section 7.1.1.6.4, Interim Revision 3 states that each PS and SAS signal processor has a CPU state switch that controls each processor's operation state.

**Figure 7.9-1 Interface between U.S. EPR I&C Safety Systems and PICS9**



These key-operated switches are located in the associated processor's TXS cabinet. The key-operated switches prevent alteration of modifiable parameters and changes to software from the SU, except when the processor is placed in the proper operational state for the change. TXS processors can be in one of four operating. To change the operating state of a safety-related CPU:

1. The CPU state switch is positioned to the desired mode
2. The SU sends a request to change states
3. The CPU receives the request and verifies the CPU state switch position
4. The CPU enters the desired operating state

FSAR Tier 2, Section 7.1.1.5.14, Interim Revision 3 mark-ups, states that a dedicated SU is also provided to for testing and maintenance of the Rod Position and Measurement System. This section states that each division of the RPMS has a MSI for testing and maintenance of the RPMS. Each MSI connects to a dedicated SU for the RPMS, which resides in the I&C service center. The RPMS MSI does not have any other connections than to its dedicated SU. The SU connections to the MSI are implemented in the same manner as the PS and SAS.

<sup>9</sup> Derived from FSAR Tier 2, Figure 7.1-2, Revision 3 Interim mark-ups (Note: Certain I&C systems, such as the SCDS, are not depicted.)

In a June 22, 2011, response to RAI 442, Question 07.01-31, the applicant modified the QDS classification to be non-safety related. Therefore, the access control requirement of IEEE Std 603-1998, Clause 5.9, does not apply to the SICS QDS.

The computer terminals for the SUs are located in the I&C service center. Topical Report EMF-2110(NP)(A), Section 2.6.2 describes additional access controls provided on the SU. The safety I&C, the SU, and the associated local area network are typically installed in the security area of the nuclear power plant. Therefore, all security measures on site that provide access control to this area apply by default to the SU. Additionally, access to the functions of the SU is subjected to further safety mechanisms. These primarily serve for the identification of authorized persons and furthermore for the assignment of the agreed user rights ("privileges"). The admissibility of the access to and the use of the SU are controlled in the following ways:

- Within the SU, the user rights are fixed on two levels: (1) The level of the operating system and (2) the level of the application software. On the level of the operating system, it is checked whether a user is allowed to use any services of the SU at all and, if yes, which of these services are selected.
- The user is identified in the course of "log-in" by his/her name and an associated password, whereby, together with this identification, user rights are assigned. In addition, it is checked within the application programs of the SU which service operations may be executed by the specific user, whereby the programs refer to the identification of the user by the operating system.
- Authorized operator actions are monitored by the central server of the SU.
- Independent control of the rights to use the SU, commands sent from the SU to the function processors are only executed if the function processors are in an appropriate operating mode.
- The change-over to an operating mode different from, "CYCLIC PROCESSING [operating mode]" is only possible if an additional release signal which is independent of the SU is present. This release signal has to be set in accordance with the MCR staff. It is governed by key switches and transmitted via single wires to the MSI computer of each redundant initiation train.

Topical Report ANP-10272P provides additional information on the security controls during the development of the TXS platform, as well as a description of the controls for the development environment of the U.S. EPR application software to prevent unauthorized modification to the platform and application. This topical report provides a description of the security features in the TXS system that can be used to prevent unauthorized or inadvertent access to the system during operations to address the criteria of RG 1.152, "Criteria for Use of Computers in Safety System of Nuclear Power Plants," Revision 2, Regulatory Positions C.2.1-C.2.5. Regulatory Positions C.2.1 - C.2.5 provide criteria for the protection of digital safety systems and establishment of secure development and operating environment for those systems. The evaluation of the access controls provided for the development environment of the TXS system, as well as the security features provided in the system design to address RG 1.152, Regulatory Positions C.2.1-C.2.5, are included in the safety evaluation report for this topical report. A summary of this evaluation is provided in Section 7.1.4.7 of Topical Report ANP-10272P.

Based on FSAR Tier 2, Interim Revision 3 mark-ups, provided in a June 22, 2011, response to RAI 442, Question 07.01-26, the staff finds the proposed modifications to include a hardwired disconnect with a physical isolation switch is adequate to prevent unauthorized changes and access to the safety system via the SU. The staff finds that based on the fact that only a single key may operate the isolation switch for all eight hardwired disconnects and that the isolation switch physically retains the key, the SU can only access one division at a time, which prevents a failure within the SU or the data communication path from affecting the SAS/PS within multiple safety divisions. Although FSAR Tier 2, Section 7.1.1.5.14, Interim Revision 3, states that the connection of the dedicated SU to the MSI of the RPMS is in the same manner as the PS and SAS, the staff determined that the applicant has not described how the principle of key retention extends to the isolation switch that connects the dedicated SU to the RPMS. Therefore, in RAI 505, Question 07.09-72, the staff requested that the applicant address this issue. Specifically, if one division of the SAS/PS is connected to its SU (e.g., SAS/PS processor of Division 1), the applicant has not described what method is employed to prevent the dedicated SU for the RPMS from being connected to a separate division of the RPMS (e.g., RPMS processor of Division 2). **RAI 505, Question 07-09-72 is being tracked as an open item.**

#### 7.9.4.4 *Single Failure Criterion and Data Communications System Failure Modes*

10 CFR Part 50, Appendix A, GDC 21 requires the protection system to be designed for high functional reliability and inservice testability commensurate with the safety functions be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. In addition, IEEE Std 603-1998, Clause 5.1 requires safety systems to perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

To meet the requirements of GDC 21, and IEEE Std 603-1998, Clause 5.1, data communication systems in support of safety functions should address the single failure criterion guidance described in SRP Section 7.9. SRP Section 7.9 states that data communication systems design should ensure that channel assignments to individual communication subsystems are appropriate to assure that both redundancy and diversity requirements within the supported systems are met. In addition, the redundant divisions that communicate with each other should be independent from one another such that a single failure will not propagate to other redundant divisions.

FSAR Tier 2, Section 7.1.2.6.12 states that the safety systems within the U.S. EPR design meets the requirements of IEEE Std 603-1998, Clause 5.1. The safety systems are arranged in four independent divisions, located in four physically separated Safeguard Buildings. The major safety system within the U.S. EPR safety-related I&C systems consists of the SICS, PS, SAS, and PACS. In RAI, 442, Question 07.01-26, the staff requested the applicant to provide sufficient information for the staff to conclude that the safety-related standalone or packaged systems provide sufficient independence between those standalone systems and other safety or non-safety systems. As described in a June 22, 2011, response to RAI 442, Question 07.01-26, the SCDS and RPMS will be added as a new safety I&C system in the U.S. EPR design. The

June 22, 2011, response to RAI 442, Question 07.01-26 includes mark-ups to FSAR Tier 2, to reflect this change. The SICS, RPMS, SCDS, PS, SAS, and PACS are each organized into four independent divisions. With the exception of the PACS, data communication or hardwired interfaces exist between redundant divisions of these safety systems through hardwired connections. The SICS provides an interface between the operators and the automation systems. The SCDS receives hardwired signal inputs from sensors or black boxes and sends hardwired signal outputs to the SICS, DAS, PS, SAS, RCSL, and PAS, as needed. The PS and the SAS acquire and process sensor information from the SCDS to perform automatic system control functions and transmit information for display to the operator, as well as communicating with non-safety systems for monitoring purposes. The PACS prioritizes the actuation requests from the PS, SICS, SAS, and non-safety related DAS and PAS, and actuates the Engineered Safety Features equipment accordingly. The RPMS measures the position of a RCCA located in the reactor vessel and provides the measurement to the DCS for control and indication to the operator. The PS and SAS provide inputs to the PACS using hardwired connections. Table 7.9-2 of this report provides a summary of the implementation of data communication and hardwired interfaces for the U.S. EPR safety I&C systems. A discussion of the communication network architecture within the PS and SAS is provided below.

**Table 7.9-2 Summary of Data Communications Implementation for Safety Systems**

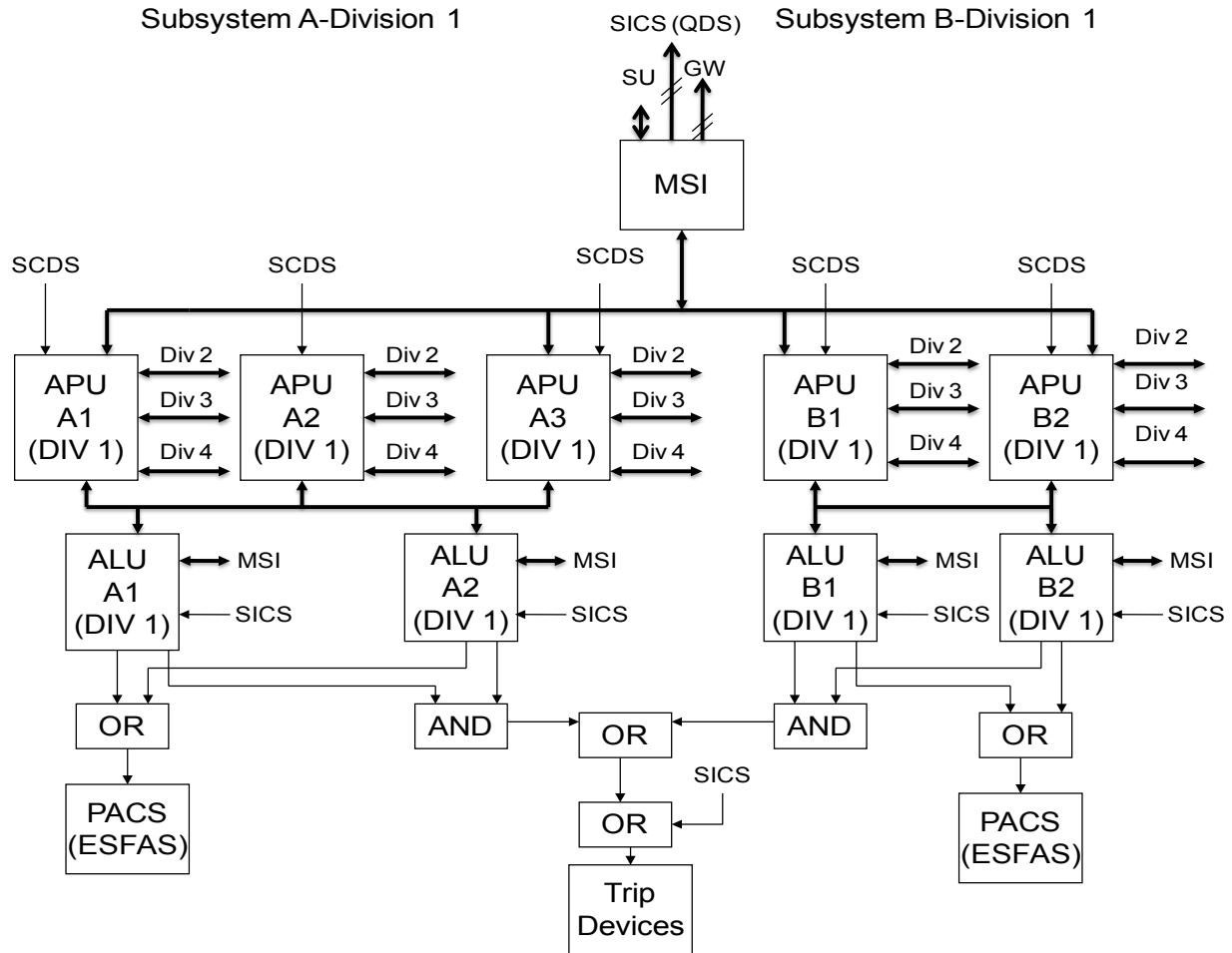
<b>Interfaces</b>	<b>Type</b>	<b>Protocol</b>
SICS-PS (control)	Hardwired	N/A
SCDS-SICS (monitoring)	Hardwired	N/A
SAS-SICS (control)	Hardwired	N/A
PS-PACS	Hardwired	N/A
SAS-PACS	Hardwired	N/A
MSI (SAS)-SICS (monitoring)	Hardwired	N/A
SICS-PACS	Hardwired	N/A
PS-TG I&C	Hardwired	N/A
CU-CU (within SAS)	Bi-directional, Point-to-Point network	SINEC Profibus
CU-MSI (within SAS)	Bi-directional, Point-to-Point network	SINEC Profibus
APU-ALU (within PS)	Bi-directional, Point-to-Point and Ring network	SINEC Profibus
MSI-MU-APU (within PS)	Bi-directional, Point-to-Point and Ring network	SINEC Profibus
MSI-MU- ALU – MSI-AU (within PS)	Bi-directional, Ring network	SINEC Profibus
RPMS-SU	Bi-directional, Point-to-Point	SINEC Profibus

#### *7.9.4.4.1 Protection System*

Technical Report ANP-10309P, Revision 3, Section 6 provides a description of the communication network topology within PS. In general, two types of Class 1E data communications network connections are utilized within the PS. These are redundant point-to-point and redundant ring network connections. Bi-directional communication is implemented for both types of network connections. A summary of these two types of network topologies is provided below. Technical Report ANP-10309P, Figure 6-3 through Figure 6-12 depicts the network architecture within the PS architecture, implemented using individual point-to-point and ring networks. These figures are designated proprietary. This technical report states that these represent the intended PS network design. These figures are provided to assist in understanding general network concepts described in this technical report, but are subject to modification during the U.S. EPR detailed design process. In RAI 442, Question 07.09-63, the staff requested that the applicant clarify how the general network concepts described in this technical report may be modified. In a February 25, 2011, response to RAI 442, Question 07.09-63, the applicant stated that the statement in Technical Report ANP-10309P, Section 6 regarding the potential modification to the general network concepts and diagrams will be deleted for clarification purposes. The staff finds this response adequate and the staff has verified the appropriate modification in Technical Report ANP-10309P, Revision 3. The verification that logical connections meet the reactor trip and engineering safety feature actuation sequence is to be completed during the inspection of the detailed PS hardware and software design and implementation. Figure 7.9-2 of this report provides an illustration of the logical connections within the PS architecture for one division. Section 7.3.4.2 of this report provides a high-level description of the individual PS units depicted in Figure 7.9-2 below, including the Acquisition and Processing Unit and Actuation Logic Units. Section 7.1 of this report also provides a description of the two subsystems within each division of the PS.

Technical Report ANP-10309P, Revision 3, Sections 7.2 and 8.2 discuss how the reactor trip voting logic and ESF actuation voting logic, respectively, are adjusted when single failures upstream of the ALU layer result in invalid signal received at the ALU. In the case of the reactor trip, the voting logic is modified such that if one faulty input signal is received, the voting logic is changed to 2 out of 3 and if two faulty input signals are received the logic is changed to 2 out of 2. If more than two faulty input signals are received, the voting logic is modified as actuation. In the case of the ESF actuation voting logic, the voting logic is changed to 2 out of 3 if one faulty input signal is received and if two faulty input signals are received the logic is changed to 2 out of 2. If more than two faulty input signals are received, the voting logic is modified as no actuation. The review of the modification to the voting logic of the reactor trip and ESF actuation functions is evaluated in Section 7.1 of this report. Technical Report ANP-10309P, Revision 3, Section 7.3 describes how invalid signals are identified. The specific details in this Section regarding how invalid signals are identified are deemed proprietary. To summarize, in the case of communication failures, the receiving computer will mark a message as invalid (faulty status) if errors are detected in the received message (e.g. incorrect message length, format, age).

**Figure 7.9-2 Depiction of Logical Connections within One Division of PS**



This detection occurs at the communication processor before the individual signals are extracted from the message. Therefore, if a received message is faulty, the faulty status is already attached to the signal in the message prior to being used by the function processor.

#### Point-to-Point Network Topology

A redundant point-to-point network topology consists of two Optical Link Modules (OLMs) and two double fiber-optic links between them. Each double fiber optic link consists of a separate transmit and receive channel. The OLM propagates messages to other OLMs on a given network. When an OLM receives a message via any channel, the message is forwarded to the other channels for transmission. In this topology, a break in one of the double fiber optic connections or a failure in one optical port of the OLM does not affect network availability. If an OLM is lost, the affected network becomes unavailable, but the redundant divisions of the PS allow the safety function to be performed through other unaffected networks. Technical Report ANP-10309P, Figure 6-1 depicts the point-to-point network. The specific implementation of the PS architecture using point-to-point topology is proprietary.



## Ring Topology

A redundant ring network topology consists of at least three OLMs and their corresponding double fiber optical links. A given redundant ring network topology can contain only a finite number of OLMs. Each network in the PS contains fewer OLMs than the maximum allowed. Each double fiber optical link consists of a separate transmit and receive channel. In this topology, a break in one of the double fiber optical connections, or a failure in one optical port of one OLM, does not affect network availability. If an OLM is lost, only the unit(s) directly connected to the failed OLM is affected. The remaining units accessing the ring network can still communicate with one another. Technical Report ANP-10309P, Figure 6-2 depicts a ring network. In the PS design, data communication using the redundant ring network involve a maximum of two divisions. The specific implementation of the PS architecture using the ring network is proprietary.

Technical Report ANP-10309P, Revision 3, Section 6 states both the point-to-point and redundant ring network topology are used to interconnect APUs of one division to other redundant divisions. In addition, the ring network is also used for communication between the MSI and each APU, as well as interconnecting the MSI-Main Unit (MU), APU, ALU, and MSI-Auxiliary Unit (AU).

### *7.9.4.4.2 Safety Information and Control System*

RAI 442, Question 07.01-31 requested the applicant to provide information which adequately describes the commercial grade dedication program for the SICS QDS and the associated critical characteristics. The applicant's June 22, 2011, response to RAI 442, Question 07.1- 31, states that FSAR Tier 2, Section 7.1.1.3.1 will be modified to reflect the new SICS design. This response states that the SICS will implement dedicated hardwired I&C for safety control and indication functions. The SICS controls and indications interface with other safety components using hardwired connections. In addition, a subset of plant parameters is duplicated on the non-safety-related QDS for situational awareness. The QDS receives input from the four divisions of the PS. Data communication isolation between the PS and the non-safety-related QDS is provided by the PS.

### *7.9.4.4.3 Safety Automation System*

FSAR Tier 2, Section 7.1.1.4.2, Interim Revision 3 mark-ups, provided in a June 22, 2011, response to RAI 442, Question 07.01-26 states that Control Units execute the logic for the assigned automatic and manual grouped control functions within the SAS. Multiple sets of redundant CUs may be provided within each division. Redundant CUs in multiple divisions may have interdivisional communication between them to perform their functions. CUs communicate with other CUs using bi-directional, point-to-point data connections implemented with the TXS Profibus protocol. The SAS functions that require interdivisional communication were provided in a May 20, 2011, response to RAI 442, Question 07.9-64 and will be discussed in subsequent sections of this safety evaluation. Interdivisional data communication is implemented in these cases to support voting functions to prevent single failure from resulting in loss of safety functions. The CUs acquire hardwired inputs from the SCDS, PS, or SICS via hardwired connections. Outputs may also be sent to the PAS to coordinate logic for related actuators. Outputs from the CUs are sent to the PACS for signal prioritization and drive actuators. Data is sent from the CUs to the hardwired I&C indications on the SICS via the MSI, or via the MSIs and redundant GWs for display on PICS.

#### *7.9.4.4.4 Evaluation of Data Communications Single Failure Protection*

Based on the staff's evaluation of the information presented in FSAR Tier 2, Chapter 7, as supplemented by Technical Report ANP-10309P, the staff finds the applicant has adequately demonstrated that the data communication systems in support of U.S. EPR safety systems meet IEEE Std 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21, by providing sufficient redundancy or alternative means to prevent loss of safety functions due to a single failure. The specific details of the staff's review regarding the SICS, PS, and SAS data communication to meet the requirements of IEEE Std 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21 is summarized below. Since PACS and SCDS do not use data communication between redundant safety divisions, these two systems were not included in this evaluation.

#### **SICS**

As a result of the proposed modification to the SICS design to change the QDS to non-safety-related and the inclusion of hardwired I&C to support control and indication functions, the proposed SICS design will not contain any safety-related data communication links or interfaces. Therefore, the staff finds that the requirements of IEEE Std 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21 are not applicable to the SICS functions due to their hardwired connections.

#### **PS**

In the case of the PS, the staff finds the redundant divisions of the PS can adequately perform the required safety functions if a single failure occurs in the data communication for both the point-to-point and ring network topology. Specifically, since the PS has four redundant divisions, a single failure within the point-to-point network will only affect a maximum of two divisions. This is also the case for the redundant ring network since data communication, using the redundant ring network involve a maximum of two divisions. Therefore, the remaining unaffected two divisions will be able to perform the safety function. In addition, the staff finds the use of error detection and invalid signal identification is adequate to preclude faulty data message from adversely impacting the function processors in the receiving division. The staff finds that given the four division redundancy provided for the PS, if a PS division or its associated data communication components are out of service for maintenance or testing, there is sufficient redundancy in the remaining three divisions to meet the single failure criterion. Furthermore, the staff finds use of watchdog timers to disconnect the load power supply for the Input/Output modules if the watchdog timer times out adequate to address unexpected failures in the ALU. As stated in Technical Report ANP-10309P, Revision 3, Section 7.4, a PS output of zero-voltage will actuate the RT. Thus, when the watchdog timer times out, the output of the PS will be set to zero which causes the reactor trip devices to de-energize. The detailed description and evaluation of the watchdog timer is in Topical Report EMF-2110(NP)(A), Section 2.4.3.4.2 and Technical Report ANP-10309P, Revision 3, Section 2.2.1.2, respectively. As such, the staff finds the data communication system that supports the PS functions is adequate to satisfy the requirements of IEEE Std 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21.

#### **SAS**

Based on the redundancy and independence provided within the SAS design the staff finds that given a single failure within one division of the SAS, the remaining interconnected SAS divisions have sufficient redundancy to maintain the safety function. Specifically, since each division has multiple redundant CUs whose outputs are arranged in an "OR" configuration, a failure of one

CU will not prevent the redundant CUs in the division from accomplishing their safety function. In addition, since the CUs of one division interface with other divisions only through point-to-point connections, a failure of one division will at most affect two divisions, therefore, the remaining two divisions can accomplish the safety function. The staff finds that given the four division redundancy provided for the SAS, if a SAS division or its associated data communication components are out of service for maintenance or testing, there is sufficient redundancy in the remaining three divisions to meet the single failure criterion. Therefore, the staff finds that the SAS data communication functions meet the requirements of IEEE Std 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21.

#### 7.9.4.5 *Data Communication System Failure Modes*

10 CFR Part 50, Appendix A, GDC 23, "Protection System Failure Modes," requires the protection system to be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced. NUREG/CR-6082, "Data Communications," provides additional discussion of independence and failure modes.

The applicant provided a list of communication faults that are mitigated for the PS in Technical Report ANP-10309P, Appendix A, Revision 3, Table A.1-1. This table also provides TXS network mitigation techniques for these communication faults and applies to all TXS-based systems. The postulated communication failures are based on the failures described in Digital Instrumentation and Control System Interim Staff Guidance-04 (D I&C ISG-04) Section 1, "Interdivisional Communications," Criterion 12. D I&C ISG-04 states that these credible communications may include, but are not limited to the following:

- Messages may be corrupted due to errors in communication processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
- Messages may be repeated at an incorrect point in time.
- Messages may be sent in the incorrect sequence.
- Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
- Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
- Messages may be inserted into the communication medium from unexpected or unknown sources.
- Messages may be sent to the wrong destination, which could treat the message as a valid message.
- Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.

- Messages may contain data that is outside the expected range.

The mitigation measures utilize a combination of CRC validation for message integrity, pre-defined message types and length, deterministic data communication, and message age to ensure that postulated communication failures do not adversely impact the PS such that the PS fails into an unsafe or unacceptable state. Additionally, in RAI 56, Question 07.08-16, the staff requested that the applicant demonstrate how a failure of the OLM will not adversely influence the signal such that the failure will not propagate to other equipment on the same data link, as described in RAI 56, Question 07.09-16. In their March 3, 1009, response, the applicant stated in "Response to Request for Additional Information No. 56, Supplement 3," that a safety-related design function of each OLM in a network is to correctly propagate data messages, while a safety-related design function of each function processor is to detect and disposition invalid received messages. Application of the single failure criterion dictates that a postulated failure of an OLM resulting in an invalid message, concurrent with a failure of a receiving unit to detect the message as being invalid, is beyond the design basis of the system. An error caused by an OLM in the sending division will propagate to the receiving division. However, if the receiving entity does not recognize and accommodate the error, then communication independence is compromised. When analyzing an OLM failure, communication independence is only compromised by a postulated failure of both the OLM in the sending division and the function processor in the receiving division. Based on the information provided by the applicant in their response to RAI 56, Question 07.9-16, described above, and the methods described in Table A.1-1 to mitigate data communication errors, the staff finds TXS data communication error handling methods ensure that the TXS data communication system meet the requirements of 10 CFR Part 50, Appendix A, GDC 23.

#### 7.9.4.6 *Independence*

##### 7.9.4.6.1 *Independence Between Redundant Portions of the Safety System*

IEEE Std 603-1998, Clause 5.6.1, requires redundant portions of the safety system to be independent and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function. SRP Appendix 7.1-C, provides acceptance criteria for the requirements of IEEE Std 603-1998. Section 5.6 of Appendix 7.1-C states that three aspects of independence should be addressed, including physical independence, electrical independence, and communication independence. Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," describes an acceptable method for complying with the NRC regulations with respect to the physical independence requirements of the circuits and electrical equipment that comprise or are associated with safety systems. RG 1.75 endorses IEEE Std 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits" as an acceptable method for satisfying the regulatory requirement concerning physical independence of circuits and electrical equipment that comprise safety systems. SRP BTP 7-11 provides guidance on application and qualification of isolation devices used to ensure electrical independence for safety systems. In addition, D I&C ISG-04, Revision 1, dated March 6, 2009 (ADAMS Accession Number ML083310185) provides acceptance criteria for communication and functional independence between redundant divisions of safety systems.

#### Physical Separation and Electrical Isolation

The evaluation of physical separation and electrical isolation requirements to meet the requirements of IEEE Std 603-1998, Clause 5.6.1, is provided in Section 7.1.4.10 this report.

## Communication Independence

Section 7.1.1.6.4 of the U.S. EPR FSAR Tier 2, Interim Revision 3, as provided in their June 22, 2011, response to RAI 442, Question 07.1-26, states that the PS and SAS implement interdivisional communication to support the system functional requirements. Communications independence is provided by the following features of the TXS platform:

- Communication modules are provided separate from the function processors performing the safety function.
- Communication are implemented with separate send and receive data channels.
- Asynchronous, cyclic operation of the function processors and communication modules.

In addition, only predefined messages are accepted by the receiving function processor, and data integrity checks are performed on the received messages. Faulted messages are flagged and ignored in subsequent logic.

During the June 25, 2010, public meeting with the applicant, the staff informed the applicant that the I&C systems design has not been demonstrated to meet NRC requirements on independence for both data communication between redundant safety divisions and between safety and non-safety systems. Specific areas of concern include:

1. Complexity of design
2. Data communication between safety divisions
  - a) Between SICS divisions
  - b) Between SAS divisions
  - c) Between PS divisions
- 3) Continuous connection between non-safety SU and safety division
- 4) Data communication from non-safety PICS to safety divisions

For data communication between redundant safety divisions in the original design, the staff emphasized that since each redundant PS division share the same set of Self-Powered Neutron Detector sensor measurements via ring networks for the High Linear Power Density and Departure from Nucleate Boiling Ratio reactor trip functions, the redundant PS divisions must rely on information from outside divisions. In addition, within the SAS, each division relied on information from outside the division to support sensor signal selection functions. Relying on information from outside the safety division is in contrast to the requirement of IEEE Std 603-1998, Clause 5.6.1. Therefore, the staff determined that the design did not meet the requirements of IEEE Std 603-1998, Clause 5.6.1 for independence between redundant divisions.

In response to the June 25, 2010, public meeting, on July 28, 2010, the applicant submitted a Closure Plan for the U.S. EPR Instrumentation and Control Communication Independence Issues. Revision 4 of this Closure Plan states that the SICS panel interfaces interdivisional communication will be eliminated. Interdivisional data communication between SICS divisions

are completely eliminated through the use of hardwired I&C for safety indications and controls, as described in a June 22, 2011, response to RAI 442, Question 07.01--31.

For the PS, the Closure Plan states that each of the 72 SPND measurements will be hardwired to each division of the PS prior to processing by PS computers. In this way, each division of the PS can perform its calculations based on all 72 SPND measurements without transmitting SPND measurements between PS divisions via networked data communication. In addition, the applicant submitted an alternative request pursuant to 10 CFR 50.55a(a)(i) to use the same 72 SPND measurements in the four PS divisions in lieu of the independence requirements for redundant divisions in IEEE Std 603-1998, Clause 5.6.1. Attachment 2 of the Alternative Request states that the applicant requests the use of conservative setpoint selection method to satisfy single failure requirements for the SPND-based reactor trip functions as an alternative to independence between redundant divisions, as required by IEEE Std 603-1998, Clause 5.6.1. IEEE Std 603, Clause 5.6.1 is identical in both the 1991 and 1998 versions of IEEE Std 603. The applicant requested the use of the 1998 in lieu of the 1991 version of this standard in a separate alternative request. The Alternative Request, Attachment 2, Section 2.0 describes the benefits of the use of SPND based core surveillance and justification to pursue an alternative to meeting the requirements of IEEE Std 603-1998, Clause 5.6.1. The evaluation of the alternative request is in Section 7.1.4.1 of this report.

Technical Report ANP-10309P, Revision 3, incorporated the proposed changes to the PS architecture to reflect the hardwired SPND measurements. Technical Report ANP-10309P, Revision 3, provides a description of the interdivisional communication between function computers of different divisions within the PS. This technical report states that the hardware configuration within the PS includes a function computer with a Profibus communication module attached. Each communication module is connected to an OLM that converts the electrical communication signals to optical signals, which are transmitted over fiber-optic cables to other OLMs on the network.

Technical Report ANP-10309P, Revision 3, Section 11 states that communication activities are performed sequentially and controlled by the central control unit of the run-time environment. The sending function computer initiates sending activities and the messages are addressed to the receiving function computer. The intermediate communication modules and OLMs transfer the messages without influencing the message data. This section also states that the TXS communication techniques provide communication independence, by using buffering circuits between redundant divisions, and are consistent with the guidance of IEEE Std 7-4.3.2-2003. For communication between redundant divisions in the PS, the buffering circuit consists of the Profibus controller and DPRAM, both contained in the communication module. The communication module provides buffering so the function computers can read and write to the DPRAM independently of the Profibus controller, which transfers data between the network and the DPRAM. Therefore, the function computer in one division operates independent of the operation of a function computer in a redundant division. Data transmission is always performed in the following manner:

- The function processor writes data to be transmitted into the interface module DPRAM.
- The data is transmitted via the applicable network and protocol to the interface module of the receiving function processor or system.

- The receiving interface module writes the data into the receiving function processor DPRAM. The receiving function processor reads the data from its DPRAM and checks the data integrity.

Technical Report ANP-10309P, Figure 11-3 depicts the use of buffering circuits and separation of data flow for communication isolation between two function computers of different divisions.

For the SAS, the Closure Plan states that three types of SAS functions will utilize data communication between divisions,

- Automatic control functions where sensor measurements are sent between divisions, and the 2nd max/2nd min measurement is selected for use in each division.
- Automatic actuation functions where binary signals are sent between divisions for voting logic or to maintain mechanical train and electrical division alignment.
- Human system interface functions where binary signals are sent between divisions for manual control purposes or sensor measurements are sent between divisions for consolidation on one video display for monitoring purposes.

During an audit of the FSAR Tier 2, Chapter 7 design developments, the staff informed the applicant that significant information is required to justify why the 2nd max/2nd min function enhances plant safety to meet D I&C ISG-04, Section 1, Criterion 3. Specific details of the staff's findings during the audit are documented in, "Audit Report for December 8-10, 14 and 20, 2010: An Audit to Review the U.S. EPR Final Safety Analysis Report Chapter 7 Design Change Development." In response to the staff's findings, the applicant modified the SAS design to preclude the use of 2nd max/2nd min measurements. The applicant also included a list of all SAS functions in FSAR Tier 2, Table 7.1-5, Interim Revision 3, which was provided as part of a June 22, 2011, response to RAI 442, Question 7.1-26. Of the SAS automatic functions listed in FSAR Tier 2, Table 7.1-5, 25, functions use interdivisional communication between redundant SAS divisions to accomplish the safety function. These functions are required to support safety functions (e.g., isolation, component trip, control, interlock, switchover functions) in the component cooling water system, main steam system, in containment refueling water storage tank system, safety chilled water system, safety injection and residual heat removal system. These functions are accomplished through the use of discrete data types and voting functions. Furthermore, FSAR Tier 2, Section 7.1.1.4.2, Interim Revision 3 states that redundant pairs of CUs that perform functions requiring interdivisional communication identified in FSAR Tier 2, Table 7.1-5 have data communication between CUs in different divisions. For those redundant pairs of CUs that do not have any functions allocated that require interdivisional communication, there are no data connections between redundant pairs CUs in different divisions.

FSAR Tier 2, Figure 7.1-7, Interim Revision 3 was modified to show point-to-point communication between different divisions of the SAS CUs. In addition, as a result of the proposed modification to use hardwired I&C for safety indication and controls in the SICS design, as described in a June 22, 2011, response to RAI 442, Question 07.01-26, SAS interdivisional communication to support human system interface functions has been removed.

Based on the information provided in FSAR Tier 2, Chapter 7, Interim Revision 3, the staff finds that since the safety-related portion of the SICS composes of hardwired I&C and therefore does not use data communication between redundant SICS divisions, the SICS does not need to meet the data communication independence requirements of IEEE Std 603-1998, Clause 5.6.1.

Based on the information provided in FSAR Tier 2, Chapter 7, Interim Revision 3, the staff finds that the SAS data communication has not fully addressed the communication independence requirements of IEEE Std 603-1998, Clause 5.6.1. The staff evaluated the SAS interdivisional communication functions using the 20 criteria in D I&C ISG-04, Section 1 as shown in FSAR Tier 2, Table 7.9-3, and determined that the SAS has not adequately addressed D I&C ISG-04, Criteria 2 and 12. Specifically, the staff determined that the applicant has not provided sufficient detail regarding provisions in the design that prevents SAS divisions from being adversely impacted by information originating from outside the division. Therefore, in RAI 505, Question 07.09-71, the staff requested that the applicant clarify how invalid signals are identified by SAS processors and state whether the voting logic in the SAS is modified to accommodate the identified invalid signals. **RAI 505, Question 07.09-71 is being tracked as an open item.** The staff finds that the interdivisional communication does support the enhancement of safety functions since the SAS functions, including those that implement interdivisional communication, are only used to support the performance of safety functions, as specified in FSAR Tier 2, Table 7.1-5.

Based on the information provided in Technical Report ANP-10309P, Revision 3, the staff finds that adequate communication independence exist between redundant portions of PS to meet the communication independence requirements of IEEE Std 603-1998, Clause 5.6.1. Specifically, the staff finds that the information presented in Technical Report ANP-10309P, Revision 3 has fully addressed the 20 criteria in Section 1 of D I&C ISG-04 as shown below in Table 7.9-3 of this report.



**Table 7.9-3 Evaluation of the U.S. EPR Safety System Interdivisional Communication**

Point	Acceptability	Basis
1	The staff finds D I&C ISG-04, Criterion 1 has been satisfied.	<p>FSAR Tier 2, Interim Revision 3 mark-ups and its referenced documents demonstrate that each safety division does not require information from outside its division to accomplish its safety function with the exception of the two safety functions that use SPND measurements. This exception has been evaluated as part of the alternative request to meeting IEEE Std 603-1998, Clause 5.6.1 as described in Section 7.1.4.1 of this report. With the exception of safety functions that use the SPNDs, the redundant PS and SAS divisions do not rely on information from outside its own division to perform its safety function. In the PS, voting logic supports reactor trip and ESF safety functions. In the SAS, voting logic is used to support isolation, interlock, switchover, and safety control functions. Since a voting scheme is used for these safety functions, and any partial trigger or ESF actuation function is accomplished prior to the voting function, the staff concludes that a safety division is not dependent on information from outside its safety function to accomplish the safety function.</p>
2	The staff finds D I&C ISG-04, Criterion 2 has not been fully satisfied.	<p>FSAR Tier 2, Interim Revision 3 mark-ups and its referenced documents have not demonstrated how SAS divisions are protected from adverse influence from outside its own division. Although each SAS division only receives discrete data from redundant SAS divisions for voting purposes, the information presented does not discuss how invalid signals are identified by SAS processor or state whether the voting logic in the SAS is modified to accommodate the identified invalid signals. The staff requested this information in RAI 505, Question 07.09-71. <b>RAI 505, Question 07.09-71 is being tracked as an open item.</b></p> <p>The staff finds FSAR Tier 2, Interim Revision 3 mark-ups and its referenced documents have demonstrated how PS divisions are protected from adverse influence from outside the division. For the PS, since each division receives data from redundant divisions for voting purposes, the division is protected from any spurious or missing data received from outside its division. In addition, communication failures will be detected, as described in Section 7.9.4.4.2 of this report and will be accommodated through identifying invalid signals received in the communication processor and using voting logic modification to accommodate the identified invalid signals. Therefore, each PS division will not be adversely influenced by information received outside its safety divisions.</p>

Point	Acceptability	Basis
3	The staff finds D I&C ISG-04, Criterion 3 has been fully satisfied.	<p>The staff finds that FSAR Tier 2, Interim Revision 3 mark-ups and its referenced documents have fully demonstrated that information received from outside the safety division enhances the safety functions in the case of the PS. Specifically, Technical Report ANP-10309P, Revision 3, states that interdivisional communication between the redundant divisions of the PS, are for voting purposes only. Two-out-of-four and three-out-of-four voting protects against the effects of a single-failure in a division. As such, the staff finds that interdivisional communication between redundant portions of the PS enhances safety functions by supporting voting function, which is used to ensure that the PS can perform its safety function given a single failure of one PS division concurrent with another PS division out of service for testing/maintenance.</p> <p>The staff finds that FSAR Tier 2, Interim Revision 3 mark-ups and its referenced documents have demonstrated that information received from outside the safety division enhances the safety functions in the case of the SAS. Specifically, the staff finds that since interdivisional communication is only used to support the performance of safety functions support isolation (i.e., interlock, component trip, switchover, and safety control functions), as specified in FSAR Tier 2, Table 7.1-5, D I&amp;C ISG-04, Section 1, Criterion 3, has been adequately addressed.</p>
4	The staff finds D I&C ISG-04, Criterion 2 has been satisfied.	FSAR Tier 2, Section 7.1.1.6.4 states that the TXS platform uses separate communication modules from function processors that operate asynchronously to each other. In addition, Technical Report ANP-10309P, Revision 3, states that the function processor only accesses shared information with the communication module only through the DPRAM.

Point	Acceptability	Basis
5	The staff finds D I&C ISG-04, Criterion 5 has been satisfied.	As stated in Topical Report EMF-2110(NP)(A), the typical cycle time of 50 ms is assumed so that the time delay between analog input and digital output to the switchgear is 50 or 100 milliseconds (ms) for a single-level configuration or 150 till 300 ms for a three-level configuration. This information is supplemented by Technical Report ANP-10309P, Appendix B, Revision 3, which shows the bounding function processor cycle time for a functional unit of the PS to be 50 ms. The staff finds the analysis provided Technical Report ANP-10309P, Appendix B acceptable to demonstrate that the bounding response times in FSAR Tier 2, Table 15.0-7, "Reactor Trip Setpoints and Delays Used in the Accident Analysis," and Table 15.0-8, "Engineered Safety Features Functions Used in the Accident Analysis," are met by the computerized portion of the U.S. EPR protection system. In addition, if the processing cycle does not reach completion in the expected amount of time, the watchdog timer expires and puts the processor into a pre-defined fault state. Indication of this occurrence is provided by other processors on the network that recognize a loss of communication with the failed processor.
6	The staff finds D I&C ISG-04, Criterion 6 has been satisfied.	Topical Report EMF-2110(NP)(A), states that all communication between the redundant divisions of the TXS safety I&C system are cyclic without possibilities of influencing the linked communication system (independent control flow of the function processor and the communication processor). The TXS communication protocol does not require any handshaking between the safety function processor and the communication processor. Handshaking is only performed within the DPRAM of the communication processor.
7	The staff finds D I&C ISG-04, Criterion 7 has been satisfied.	The function processor only accepts predefined data sets, and uses a CRC check to ensure the integrity of the data. Faulted messages are flagged and ignored in subsequent logic.

Point	Acceptability	Basis
8	The staff finds D I&C ISG-04, Criterion 8 has been fully satisfied.	As described in Topical Report EMF-2110(NP)(A), data exchange between redundant safety divisions is done using a separate communication processor that interfaces with the safety function processor through a shared DPRAM. This communication processor determines whether the data is formatted correctly and is properly addressed to the intended destination. The safety function processor processes this data as part of the standard software loop. As such, the staff has concluded that data exchange between redundant divisions of the U.S. EPR I&C safety systems is processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving division, or any other independent division, and meets D I&C ISG-04, Section 1, Criterion 8.
9	The staff finds D I&C ISG-04, Criterion 9 has been satisfied.	In the safety-related I&C systems, DPRAM locations for storing incoming messages are predefined during application software generation. Separate, fixed memory locations are used for input (receive) and output (send) messages.
10	The staff finds D I&C ISG-04, Criterion 10 is not applicable to communication between safety divisions.	This point only applies to communication between safety and non-safety systems. As such, this point is evaluated in FSAR Tier 2, Table 7.9-4.
11	D I&C ISG-04, Criterion 11 is only applicable to communication between safety and non-safety systems for the U.S. EPR design.	FSAR Tier 2 and its referenced documents state that software modifications can only be done when the function processor is in a mode other than the operating mode (CYCLIC PROCESSING). Only data messages are sent between divisions. Command messages (which can be used to upload software or changeable parameters) are only sent from the non-safety SU, which is evaluated as part of the evaluation for communication independence between safety and non-safety systems.
12	The staff finds D I&C ISG-04, Criterion 12 has been fully satisfied.	The applicant provided information on how communication faults are mitigated for the PS in Technical Report ANP-10309P, Appendix A, Table A.1-1, Revision 3. The staff finds the description of how communication errors are accommodated for all TXS based systems acceptable to address Criterion 12.

Point	Acceptability	Basis
13	The staff finds D I&C ISG-04, Criterion 13 has been satisfied.	FSAR Tier 2, as supplemented by Topical Report EMF-2110(NP)(A) and Technical Report ANP-10309P, state that messages are checked for message validity, and message age. Faulty messages are identified and tagged. The TXS system uses fault accommodation techniques, as described in Topical Report EMF-2110(NP)(A) and Technical Report ANP-10309P, (i.e. voting logic), and thus no error correcting methods are used.
14	The staff finds the deviation to D I&C ISG-04, Criterion 14 in the U.S. EPR I&C systems design acceptable.	Technical Report ANP-10309P describes the use of a ring network instead of point-to-point connections for vital data communication functions (e.g., voting logic, sensor data acquisition, etc.). Based on the methods used to detect communication failures are described in Section 7.9.4.2.2 of this report, the staff finds that the same error detection and accommodation techniques used in the point-to-point network also apply to the ring network. The staff considered that there is a possibility that a data communication failure or a software failure within one division may propagate to other divisions on the same network. However, per the requirements of IEEE Std 603-1998, Clause 5.1, safety systems are only required to accommodate single failures. Therefore, if a communication or software failure is undetected by multiple divisions, this would only be the result of multiple failures on both the sending function computer and multiple receiving function computers. Since this type of failure is beyond design basis and is accommodated by the DAS to accomplish the safety function, the staff finds the proposed alternative is acceptable as a deviation to addressing D I&C ISG-04, Section 1, Criterion 14.
15	The staff finds D I&C ISG-04, Criterion 15 has been satisfied.	The TXS system uses predefined messages set at code generation, and the communication is cyclic. The communication occurs independent of updates to the data. Messages that have not changed from the previously received data are ignored by the receiving processor.
16	The staff finds D I&C ISG-04, Criterion 16 has been satisfied.	The TXS system uses watchdog timers to monitor the runtime environment of the safety and communication processors. Message age is also monitored to identify loss of communication.

Point	Acceptability	Basis
17	The staff finds D I&C ISG-04, Criterion 17 has been satisfied.	<p>FSAR Tier 2, Sections 3.11, 7.1.2.2.2, 7.1.2.2.3, and Section 7.1.2.6.15 contain commitments to complete equipment qualification on all safety-related equipment. In addition, the following ITAAC in FSAR Tier 1 provide commitments and acceptance criteria for equipment qualification:</p> <ul style="list-style-type: none"> <li>• Table 2.4.1-7, Item 4.10 for PS</li> <li>• Table 2.4.4-6, Item 4.1 for SAS</li> <li>• Table 2.4.5-3, Item 4.3 for PACS</li> <li>• Table 2.4.26-4, Item 4.4 for the RPMS</li> <li>• Table 2.4.14-2, Items 4.1 and 6.1 for Hydrogen Monitoring System</li> <li>• Table 2.4.17-3, Items 4.1 and 6.1 for Ex-core Instrumentation System</li> <li>• Table 2.4.19-3, Items 4.1 and 5.1 for In-core Instrumentation</li> <li>• Table 2.4.22-3, Item 6.1 for Radiation Monitoring System</li> </ul>
18	The staff finds D I&C ISG-04, Criterion 18 has been satisfied.	<p>Topical Report ANP-10272P described the use of the FMEA to support the determination of hazards and performance deficits. The PS FMEA is provided in Technical Report ANP-10309P, Appendix A, Revision 3. The TXS system is only designed for safety applications and unneeded functions are precluded from software code generation. Similarly, unneeded functions are not included in the design and implementation of Programmable Logic Devices or Field Programmable Gate Arrays (FPGAs) such as those used in the PACS priority module. This is verified through requirements traceability.</p>
19	The staff finds D I&C ISG-04, Criterion 19 has been satisfied.	<p>The TXS system is designed to operate with a constant bus load. The use of token passing in the Profibus protocol verifies that only one communication processing is sending information on the network to prevent collision. In addition, FSAR Tier 2, Table 2.4.1-7, Protection System ITAAC, Item 4.24 provides response time analysis and testing acceptance criteria. This ITAAC requires the identification of the required response time from sensor to ALU output to support the safety analysis response time. This ITAAC also requires that PS response time analysis and tests confirm the response time limits for the RT signals listed in FSAR Tier 2, Table 2.4.1-2 and ESF signals listed in FSAR Tier 2, Table 2.4.1-3.</p>
20	The staff finds D I&C ISG-04, Criterion 20 has	<p>As stated in Topical Report EMF-2110(NP)(A), the typical cycle time of 50 ms is assumed so that the time delay between analog input and digital output to the</p>

Point	Acceptability	Basis
	been satisfied.	<p>switchgear is 50 or 100 ms for a single-level configuration or 150 till 300 ms for a three-level configuration. This information is supplemented by Technical Report ANP-10309P, Appendix B, Revision 3, which shows the bounding function processor cycle time for a functional unit of the PS to be 50 ms. The staff finds the analysis provided Technical Report ANP-10309, Appendix B acceptable to demonstrate that the bounding response times in FSAR Tier 2, Table 15.0-7, "Reactor Trip Setpoints and Delays Used in the Accident Analysis," and Table 15.0-8, "Engineered Safety Features Functions Used in the Accident Analysis," are met by the computerized portion of the U.S. EPR protection system. In addition, FSAR Tier 1, Table 2.4.1-7, "Protection System ITAAC," Item 4.24, provides response time analysis and testing acceptance criteria. This response time test is used to verify that adequate throughput exists for the safety-related systems to satisfy the Chapter 15 response time requirements.</p>

The staff identified the following ITACC items to verify adequate communication independence exists between Class 1E and non-Class 1E equipment:

- FSAR Tier 1, Table 2.4.1-7, Item 4.4, Interim Revision 3 mark-ups, to verify communication independence is provided between the four PS divisions
- FSAR Tier 1, Table 2.4.4-6, Item 4.8, Interim Revision 3 to verify communications independence is provided between the four SAS divisions. The staff reviewed the ITAAC provided in FSAR Tier 1, Interim Revision 3 and finds that the additional information is required to verify that communications independence exists between redundant portions of safety systems. Specifically, the staff finds that the acceptance criteria for FSAR Tier 1, Table 2.4.1-7, ITAAC Item 4.17 FSAR Tier 1, Table 2.4.4-6, Item 4.9 do not verify that messages that are not pre-defined are not accepted by the safety function processor for processing. The staff finds that this feature is key to ensuring that a failure within one division will not allow non-predefined messages from propagating to other safety divisions, which may result in loss or degradation of the safety function. Therefore, in RAI 505, Question 07.09-72, the staff requested that the applicant demonstrate how this feature is verified in the as-built safety system to meet the requirements of 10 CFR 52.47(b)(1). **RAI 505, Question 07.09-72 is being tracked as an open item.**

#### Functional Independence

Functional independence is derived from IEEE Std 603-1998, Clause 5.6, requirements to ensure that redundant portions of a safety system are independent from each other to the degree necessary to retain the capability to accomplish the safety function. This is further clarified in D I&C ISG-04, Section 1, Criterion 1, which states:

The safety system should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions.

As stated above, FSAR Tier 2, Interim Revision 3 and its referenced documents demonstrate that each safety division does not require information from outside its division to accomplish its safety function with the exception of safety functions that use SPND measurements. This exception has been evaluated as part of the alternative request to meeting IEEE Std 603-1998, Clause 5.6.1 as described in Section 7.1.4.1 of this report. With the exception of safety functions that use the SPNDs, all other safety functions that use interdivisional communication are only used to support voting logic. In the PS, voting logic is used to support reactor trip and ESF safety functions. In the SAS, voting logic is used to support isolation, interlock, switchover, and safety control functions. Since a voting scheme is used for these safety functions, and any partial trip or ESF actuation function is accomplished prior to the voting function, the staff concludes that a safety division is not dependent on information from outside its safety function to accomplish the safety function. Therefore, the staff finds that the U.S. EPR I&C safety systems design meets the functional independence requirements of IEEE Std 603-1998, Clause 5.6.1.



#### *7.9.4.6.2 Independence between Safety Systems and Design Basis Events*

IEEE Std 603-1998, Clause 5.6.2, requires safety system equipment required to mitigate the consequences of a specific design basis event to be independent of and physically separated from the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. This clause specifies that equipment qualification in accordance with IEEE Std 603-1998, Clause 5.4, is one method that can be used to meet this requirement. In addition, 10 CFR Part 50, Appendix A, GDC 22, requires the protection system to be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function.

To meet the requirements of IEEE Std 603-1998, Clause 5.6.2, data communication systems in support of safety systems shall meet the equipment qualification requirements of IEEE Std 603-1998, Clause 5.4, and accordingly, provide sufficient diversity to prevent the loss of the PS. FSAR Tier 2, Section 7.1.2.6.15 states that equipment used in safety systems will be qualified using appropriate methods under the program described in FSAR Tier 2, Section 3.11. Integrated system testing is performed as part of the TXS development process described in FSAR Tier 2, Section 7.1.1.2 to verify that the performance requirements of the safety functions have been met. In addition, FSAR Tier 2, Section 7.1.2.2.11 states that requirements of 10 CFR Part 50, Appendix A, GDC 22 are met by fulfilling the requirements of IEEE Std 603-1998, Clause 5.6.

The evaluation for independence between safety systems and design basis events to meet the requirements of IEEE Std 603-1998, Clause 5.4, is documented in Section 7.1.4.8 of this report. The evaluation in Section 7.1.4.8 of this report discusses compliance to 10 CFR Part 50, Appendix A, GDC 4, which requires structures, systems, and components important to safety to be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of- coolant accidents.

#### *7.9.4.6.3 Independence between Safety Systems and Other Systems*

IEEE Std 603-1998, Clause 5.6.3, requires safety system design to be such that credible failures in and consequential actions by other systems do not prevent the safety systems from meeting the requirements of this standard. This clause is enumerated by several subclauses, as documented below. The evaluation of the U.S. EPR safety I&C systems design against the requirements of IEEE Std 603-1998, Clause 5.6.3, is completed as a part of the evaluation of each subclause. In addition, 10 CFR Part 50, Appendix A, GDC 24, requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

#### *Interconnected Equipment*

For interconnected equipment, IEEE Std 603-1998, Subclause 5.6.3.1, requires:

- Equipment that is used for both safety and non-safety functions to be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.

No credible failure on the non-safety side of an isolation device shall prevent any part of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

To address the requirements of IEEE Std 603-1998, Clause 5.6.3, SRP Section 7.9 states that interconnections between safety systems and non-safety systems should be designed such that each safety system can perform its safety function with no input or influence from the interconnected system, and that any failure of the interconnected system, failure of communication from that system or faulty data transmitted by that system cannot prevent or influence that independent safety determination. This is further clarified by the guidance in D I&C ISG-04, which provides 20 criteria for communication between safety and non-safety systems to meet the communication independence requirements of IEEE Std 603-1998, Clause 5.6.3.

As part of the evaluation of IEEE Std 603-1998, Clause 5.6.3, the staff also evaluated whether adequate functional independence exists between U.S. EPR safety systems and non-safety systems. Functional independence is derived from IEEE Std 603-1998, Clause 5.6, requirements to ensure that redundant portions of a safety system are independent from each other to the degree necessary to retain the capability to accomplish the safety function. This is further clarified in D I&C ISG-04, Section 1, Criterion 2 quoted above.

As discussed above in Section 7.9.4.6.1 of this report, during the June 25, 2010, public meeting with the applicant, the staff informed the applicant that the I&C systems design has not been demonstrated to meet NRC requirements on independence between safety and non-safety systems. The issue concerns data communication from the non-safety related PICS to safety divisions and the continuous connection of the service unit to safety divisions.

On July 28, 2010, in response to the June 25, 2010, public meeting, the applicant submitted a Closure Plan for the U.S. EPR Instrumentation and Control Communications Independence Issues. Revision 4 of this Closure Plan states that the U.S. EPR I&C systems design will be modified such that only communication from the PS and SAS to PICS will be allowed. The communication paths will be restricted so that PICS cannot send information to the PS/SAS. In addition, the Closure Plan states that the SU connection to safety divisions will be changed such that the SU will normally be disconnected from the safety divisions by a physical disconnect. When physically connected, the SU communication with the safety function processors will operate as currently designed in a bi-directional capacity.

FSAR Tier 2, Section 7.1, Interim Revision 3 mark-ups were submitted as part of a June 22, 2011, response to RAI 442, Question 07.01-26 in order to reflect the proposed changes stated in the Closure Plan. FSAR Interim Revision 3, Section 7.1.1.6.4 states that Class 1E communication independence is provided between the PS and SAS and the following non-safety-related components:

- Qualified Display System (PS only)

- Gateway
- Service Unit

The connection between the MSI and the QDS is limited to one-way data communication from the MSI to the QDS. This is accomplished via a segment that is physically restricted to unidirectional communication (transmit only port connected to receive only port).

Communication independence is achieved by physically limiting communication to one way from the MSI to the QDS. The connection between the MSI and the GW is limited to one-way data communication from the MSI to the GW. This is accomplished via a segment that is physically restricted to unidirectional communication (transmit only port connected to receive only port). Communication independence is achieved by physically limiting communication to one way from the MSI to the GW. Technical Report ANP-10309P provides additional information regarding the interface between the MSI and QDS and between the MSI and GW as summarized in the discussion below. The SU is a non-safety-related, standard computer that is temporarily connected to a TXS system when needed to perform surveillances or troubleshoot. Communications independence between the MSI and the SU is verified by the following measures:

- The SU is normally disconnected. This is accomplished through a hardwired disconnect.
- The independence principles of the TXS platform, which include:

Communication modules separate from the function processors.

Communication between the function processors and communication modules are implemented with separate send and receive data channels.

The function processors and communication modules operate cyclically and asynchronous to each other.

Only predefined messages are accepted by the MSI, and data integrity checks are performed on the received messages. Faulted messages are flagged and ignored in subsequent logic.

CPU state switch prevents the modification of software when the function processor is in the operating mode.

#### Protection System Interfaces with Non-Safety Systems

For the PS, Section 12 of Technical Report ANP-10309P, Revision 3 states that the types of interfaces between PS and non-safety-related I&C systems are as follows:

- Information is exchanged between the SU and the PS for diagnostics, monitoring, and maintenance. This interface is normally disconnected and is made available only when an operator in the MCR enables the connection using a key switch.
- Information is exchanged between the PS and the PICS. The PS transfers data to the PICS for display to the operator. Electrical isolation for this interface is achieved through Class 1E isolation devices.

- Information is transferred from the PS to the PAS for time stamping of reactor trips and EFS functions and to initiate non-safety-related partial cooldown via an isolated hardwired connection.
- Information is transferred from the PS to the TG I&C for the turbine trip function via an isolated hardwired connection.

These interfaces are realized in different ways, but the following requirements are consistently applied to the safety to non-safety interface:

- Independence is maintained so that failures in a non-safety system do not prevent the performance of a safety function.
- Data communication between the non-safety system and the PS does not prevent the performance of a safety function.
- The safety system does not rely on information from a non-safety system to perform its safety functions.

These requirements are implemented using the Class 1E MSI, which is classified as safety-related. Topical Report EMF-2110(NP)(A), Section 2.5 describes the use of the MSI as an isolation device between automation computers of safety systems and non-safety systems, like the SU or GW to process computers. The MSI is dedicated to each redundant division, and each MSI can service up to 10 function processors. In the case of the PS, each safety processor within one division will be connected to non-safety systems via a single MSI.

Technical Report ANP-10309P, Revision 3, Section 12 states that for the interface between the PS and the SU, the SU provides the functions needed for monitoring, testing, diagnostics, and modifying application software. The SU access to the system is through the Class 1E MSI, which serves as the point of communication isolation between the SU and the PS units performing the safety-related protective functions. The connection between the PS and SU is normally disconnected using a disconnection switch. This connection can be enabled only by an operator in the MCR using a key switch.

Technical Report ANP-10309P, Revision 3, Section 12 also states that the interface between the PS/SAS and the PICS allows information from the PS/SAS to be displayed on the PICS through a uni-directional link. To verify unidirectional behavior, the connection between the MSI and the gateway, within the PS and SAS, will consist only of a transmit segment between the two electrical to optical converters (EOC) connecting the MSI to the gateway.

Technical Report ANP-10309P, Revision 3, Section 12.6 states that the interface between the PS and QDS will be uni-directional. To ensure unidirectional behavior, the connection between the two EOCs, will consist only of a transmit segment. There will be no physical segment connected that allows any transmittal of information from the QDS to the PS. Technical Report ANP-10309, Figure 12-2 depicts the use of the MSI and separation of data flow for communication independence between the PS and non-safety-related systems.

#### SICS Interfaces with SU

In a June 22, 2011, response to RAI 442, Question 07.01- 31, the applicant stated that FSAR Tier 2, Section 7.1 will be modified to reflect the new SICS design. FSAR Tier 2, Section 7.1.1.3.1 Interim Revision 3 mark-ups state that the SICS will implement dedicated

hardwired I&C for safety control and indication functions. The SICS I&C controls and indications interface with other safety components using hardwired connections. The independence requirements of data communication are not applicable for the hardwired SICS I&C. In addition, a subset of plant parameters is duplicated on the non-safety-related QDS for situational awareness. The QDS receives input from the four divisions of the PS. Data communication isolation between the PS to the non-safety-related QDS is provided by the PS. Since the QDS is classified as non-safety-related, the independence requirements of IEEE Std 603-1998, Clause 5.6.3 does not apply to the interface of the QDS and the SU.

#### PACS Interface with PAS

FSAR Tier 2, Section 7.1.1.6.4, states that data connection exists between the PAS and the PACS. However, this connection is only between the PAS and non-safety-related PACS communication module. Connections between the communication module and safety-related priority module are hardwired. The communication module is qualified as an associated circuit.

#### Evaluation of Independence Between Safety Systems and Other Systems

Based on the staff's evaluation of the data communication between safety systems and non-safety systems within the I&C architecture, the staff determined the applicant has not fully met the requirements of IEEE Std 603-1998, Clause 5.6.3, and GDC 24. Specifically, the staff determined that the information presented in FSAR Tier 2, Chapter 7, as supplemented by Technical Report ANP-10309P, Revision 3, have not fully addressed the 20 criteria within D I&C ISG-04 for data communication between safety and non-safety systems, as documented in FSAR Tier 2, Table 7.9-4.

Since interfaces between the PS and the TG I&C or PAS are hardwired, the communication independence requirements of IEEE Std 603-1998, Clause 5.6.3 are not applicable. However, these interfaces have been evaluated against the electrical isolation and physical separation requirements of IEEE Std 603-1998, Clause 5.6.3, as documented in Sections 7.1.4 of this report.

**Table 7.9-4 Evaluation of Data Communication between Safety and Non-safety Systems**

Point	Acceptability	Basis
1	The staff finds D I&C ISG-04, Criterion 1 has been satisfied.	FSAR Tier 2, Interim Revision 3 mark-ups and its referenced documents have demonstrated that each safety division does not require information from non-safety systems to accomplish its safety function. All data communication between safety and non-safety systems is not required to support the safety function. The PS and the SAS does not receive any information from the PICS. In addition, when the SU is connected to either the PS or SAS, the information exchanged is only for surveillance, testing, and diagnostic purpose, and is not required for the PS and SAS to perform any safety function. Cyclic communication within the PS and SAS ensures that all safety functions are performed prior to any diagnostic or surveillance tasks.
2	The staff finds D I&C ISG-04, Criterion 2 has been fully satisfied.	The staff finds that the design of the PS and SAS interface with non-safety systems as described in FSAR Tier 2, Interim Revision 3, mark-ups and Technical Report ANP-10309P are adequate to demonstrate that non-safety systems cannot adversely impact the performance of safety functions. Specifically, the staff finds that (1) the uni-directional link from the PS/SAS with the GW and the uni-directional link from the PS to the QDS, and (2) the qualification of the first EOC to be safety-related are adequate to physically prevent failures from non-safety systems from propagating to safety systems. The staff also finds the features within the MSI and the use of the hardwired disconnect between the SU and the MSI, as well as the CPU state switch are adequate to prevent failures originating in the SU from adversely impacting the safety function processors by ensuring that (1) the SU is normally disconnected from the safety through physical means, (2) the MSI prevents unknown and erroneous messages from propagating to safety systems, and (3) the CPU state switch prevents modification to the safety system while in the operating mode.

Point	Acceptability	Basis
3	The staff finds the deviation to D I&C ISG-04, Criterion 3 in the I&C systems design acceptable.	The PS and SAS do not receive information from the PICS. Although the SU interface with the PS and SAS does not directly enhance safety function, it is used to support testing, maintenance, and diagnostic functions which can enhance the reliability of the safety system. In addition, FSAR Tier 2, Section 7.1.1.6.4, Interim Revision 3, mark-ups state that the SU is only connected to a safety division to (1) Perform Technical Specification Surveillance Requirements and Actions, (2) Diagnose system faults following indication of a fault, and (3) Load new software versions needed to implement approved plant design changes. Therefore, the SU is not continuously connected to safety systems. The MSI will serve as the data communication isolation device to prevent communication failures from adversely impacting safety systems, and the isolation key switch will prevent more than one safety division from being connected to the SU. As such, the staff finds that the deviation to D I&C ISG-04, Criterion 3 in the U.S. EPR I&C systems design acceptable.
4	The staff finds D I&C ISG-04, Criterion 4 has been satisfied.	FSAR Tier 2, Section 7.1.1.6.4 mark-ups state that the TXS platform uses separate communication modules from function processors that operate asynchronously to each other. Technical Report ANP-10309P states that the function processor only accesses shared information with the communication module only through the DPRAM.
5	The staff finds D I&C ISG-04, Criterion 5 has been satisfied.	As discussed in FSAR Tier 2, Table 7.9-3, the cycle time of the TXS processors is fixed and the cycle time is based on the response time requirements in FSAR Tier 2, Chapter 15, Transient and Accident Analysis. The cycle time takes into account the network loading. Since the safety functions are processed at the beginning of the cycle and information received from non-safety systems are not required for the safety functions, only the remainder of the processor cycle is used to process information received from non-safety-related system. Furthermore, if the processors are unable to complete their cycle, the watchdog timer times out and sets the processor in a predefined state (e.g. initiate reactor trip).
6	The staff finds D I&C ISG-04, Criterion 6f has been satisfied.	The TXS communication protocol does not require any handshaking between the function and communication processor. Handshaking is only performed within the DPRAM of the communication processor. In addition, TXS-based processors are not interrupted by communication.
7	The staff finds D I&C ISG-04, Criterion 7 has	The function processor only accepts predefined data sets, and uses a CRC check to ensure the integrity of the data. Data is sent every cycle, whether it has changed

Point	Acceptability	Basis
	been satisfied.	since the previous transmission or not. Every message has the same structure and sequence. Faulted messages are flagged and ignored in subsequent logic. In the case of safety to non-safety communication, the MSI checks that only predefined data are allowed from non-safety systems to safety systems.
8	The staff finds D I&C ISG-04, Criterion 8 has been satisfied.	As described in Topical Report EMF-2110(NP)(A), data exchange between different TXS processors is done using a separate communication processor that interfaces to the safety function processor through a shared DPRAM. This communication processor determines whether the data is formatted correctly and is properly addressed to the intended destination. The safety function processor processes this data as part of the standard software loop. In addition, the MSI checks for faulted messages from non-safety systems and only allows messages that are in the predefined set to be transmitted to safety processors. As such, the staff finds that data exchange between safety and non-safety systems of the I&C systems is processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving division, or any other independent division, meets D I&C ISG-04, Section 8, Criterion 8.
9	The staff finds D I&C ISG-04, Criterion 9 has been satisfied.	In the safety-related I&C systems, DPRAM locations for storing incoming messages are predefined during application software generation. Separate, fixed memory locations are used for input (receive) and output (send) messages.



Point	Acceptability	Basis
10	The staff finds D I&C ISG-04, Criterion 10 has not been satisfied.	FSAR Tier 2, Section 7.1.1.6.4, Interim Revision 3, mark-ups state that the communication path between the SU and the divisional MSIs for the PS and SAS is isolated by hardwired disconnects while not in use. This is achieved with key-operated isolation switches located in the MCR. This allows MCR operators to monitor the position of the isolation switch. A local connection point for SU is located in the local MSI cabinet in each PS and SAS division. This local connection is also isolated by a key-operated isolation switch. The isolation switches in a system are keyed so that a single key operates the eight switches (four MCR and four local), and the key is physically retained in the switch when positioned to allow the SU connection. This prevents the connection of a SU to more than a single division of the PS or SAS. However, the staff finds that the applicant has not provided sufficient information regarding the SU connection to the RPMS to address D I&C ISG-04, Criterion 10. The staff finds that the applicant has not described how the principle of key retention extends to the isolation switch that connects the dedicated SU to the RPMS, as described in RAI 505, Question 07.09-72. Specifically, if one division of the SAS/PS is connected to its SU, the applicant has not described what method is employed to prevent the dedicated SU for the RPMS from being connected to a separate division of the RPMS. RAI 505, Question 07.09-72 is being tracked as an open item.
11	The staff finds D I&C ISG-04, Criterion 11 has been satisfied.	FSAR Tier 2, Interim Revision 3 Table 7.1-6 mark-up states that when a safety processor is adjusted to the "Diagnosis state," the SU can alter the application software of the function processor. In this mode, the safety processor will be declared inoperable for Technical Specifications and processor outputs disabled and cannot be enabled. In addition, all data messages are disabled such that no messages are sent from the CPU in diagnosis state. Receiving CPUs will respond to this as loss of communication. The staff finds that by disabling the CPU output such that no data messages are sent and by setting the CPU operability to "Inoperable" in Technical Specifications address D I&C ISG-04, Section 1, Criterion 11, which states that provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service.

Point	Acceptability	Basis
12	The staff finds D I&C ISG-04, Criterion 12 has been satisfied.	The applicant provided information on how communication faults are detected in Technical Report ANP-10309P, Appendix A, Table A.1.1. The described mitigation strategies in Technical Report ANP-10309P, Appendix A, Table A.1.1 apply to all TXS-based systems. As such, the staff finds the described mitigation strategies to address communication faults in the PS are acceptable to address D I&C ISG-04, Criterion 12.
13	The staff finds D I&C ISG-04, Criterion 13 has been satisfied.	FSAR Tier 2, Section 7.1, as supplemented by Topical Report EMF-2110(NP)(A) and Technical Report ANP-10309P states that messages are checked for message validity and message age. Faulty messages are identified and tagged. The TXS system uses fault accommodation techniques, as described in Topical Report EMF-2110(NP)(A) and Technical Report ANP-10309P, and no error correcting methods are used.
14	The staff finds D I&C ISG-04, Criterion 14 has been satisfied.	Although the safety function processors use a ring network to connect all safety processors within a division to non-safety systems via the MSI, the information exchanged between safety and non-safety I&C systems are not vital to achieve the safety functions. As such, the staff finds that the U.S. EPR safety to non-safety interface meets Criterion 14 of D I&C ISG-04, Criterion 14.
15	The staff finds D I&C ISG-04, Criterion 15 has been satisfied.	The TXS system uses predefined messages set at code generation, and the communication is cyclic. The communication occurs independent of updates to the data. Messages that have not changed from the previously received data are ignored by the receiving processor.
16	The staff finds D I&C ISG-04, Criterion 16 has been satisfied.	The TXS system uses watchdog timers to monitor the runtime environment of the safety and communication processors. Message age is also monitored to identify loss of communication.

Point	Acceptability	Basis
17	The staff finds D I&C ISG-04, Criterion 17 has been satisfied.	<p>FSAR, Tier 2, Sections 3.11, 7.1.2.2.2, 7.1.2.2.3, and Section 7.1.2.6.15 contain commitments to complete equipment qualification on all safety-related equipment. In addition, the following ITAAC in FSAR Tier 1 provide commitments and acceptance criteria for equipment qualification:</p> <ul style="list-style-type: none"> <li>• Table 2.4.1-7, Item 4.10 for PS</li> <li>• Table 2.4.4-6, Item 4.1 for SAS</li> <li>• Table 2.4.5-3, Item 4.3 for PACS</li> <li>• Table 2.4.26-4, Item 4.4 for the RPMS</li> <li>• Table 2.4.14-2 for HMS, Items 4.1 and 6.1</li> <li>• Table 2.4.17-3 for Ex-core Instrumentation System, Items 4.1 and 6.1</li> <li>• Table 2.4.19-3 for In-core Instrumentation, Items 4.1 and 5.1</li> <li>• Table 2.4.22-3 for RMS, Item 6.1</li> </ul>
18	The staff finds D I&C ISG-04, Criterion 18 has been satisfied.	Topical Report ANP-10272P described the use of the FMEA to support the determination hazards and performance deficits. The TXS system is only designed for safety applications, and unneeded functions are precluded from software code generation.
19	The staff finds D I&C ISG-04, Criterion 19 has been satisfied.	The TXS system is designed to operate with a constant bus load. The use of token passing in the Profibus protocol verifies that only one communication processing is sending information on the network to prevent collision. Since the safety functions are processed at the beginning of the cycle and information received from non-safety systems are not required for the safety functions, only the remainder of the processor cycle is used to process information received from non-safety-related system.

Point	Acceptability	Basis
20	The staff finds D I&C ISG-04, Criterion 20 has been satisfied.	As stated in Topical Report EMF-2110(NP)(A), the typical cycle time of 50 ms is assumed so that the time delay between analog input and digital output to the switchgear is 50 or 100 ms for a single-level configuration or 150 till 300 ms for a three-level configuration. This information is supplemented by Technical Report ANP-10309P, Appendix B, Revision 3, which shows the bounding function processor cycle time for a functional unit of the PS to be 50ms. The staff finds the analysis provided Technical Report ANP-10309P, Appendix B acceptable to demonstrate that the bounding response times in FSAR Tier 2, Table 15.0-7, "Reactor Trip Setpoints and Delays Used in the Accident Analysis," and Table 15.0-8, "Engineered Safety Features Functions Used in the Accident Analysis," are met by the computerized portion of the U.S. EPR protection system. In addition, FSAR Tier 1, Table 2.4.1-7, "Protection System ITAAC," Item 4.24, provides response time analysis and testing acceptance criteria. This response time test is used to verify that adequate throughput exists for the safety-related systems to satisfy the Chapter 15 response time requirements.

## Physical Separation and Electrical Isolation

For equipment in proximity of safety systems, IEEE Std 603-1998, Subclause 5.6.3.2, requires:

- Equipment in other systems that is in physical proximity to safety equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1992.

Physical barriers used to effect a safety system boundary shall meet the requirements of IEEE Std. 603-1998, Clauses 5.3, 5.4, and 5.5 for the applicable conditions specified in IEEE Std. 603-1998, Clauses 4.7 and 4.8 of the design basis.

The staff's evaluation of physical separation and electrical isolation between safety-related I&C systems and non-safety related I&C systems is discussed in Section 7.1.4 of this report.

## Single Random Failure

For effects of a single random failure, IEEE Std 603-1998, Subclause 5.6.3.3, stipulates that where a single random failure in a non-safety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure.

The staff's evaluation of the PR I&C system design against the requirements of IEEE Std 603-1998, Subclause 5.6.3.3, is documented in Section 7.1.4 of this report.

### *7.9.4.6.4 Control Systems Data Communication Functions*

10 CFR Part 50, Appendix A, GDC 13, requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. In addition, 10 CFR Part 50, Appendix A, GDC 19, requires that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Furthermore, 10 CFR Part 50, Appendix A, GDC 20, requires, in part, that the protection system is designed to initiate automatically the operation of the appropriate systems, and to sense accident conditions and to initiate the operation of systems and components important to safety.

SICS is a safety-related HMI. FSAR Tier 2, Section 7.1.1.3.1, Interim Revision 3 mark-ups describe the capabilities of the SICS to perform safety-related functions associated with the manual control of systems to achieve and maintain safe shutdown during normal and accident conditions. The PICS is a non-safety-related HMI that is normally used by the operator to monitor and control process systems. FSAR Tier 2, Section 7.1.1.3.2 describes the functionality of the PICS with regards to the capability for safe operation of the plant from the MCR during

normal and accident conditions. In addition, FSAR Tier 2 Section 7.5.2.1.2 states that the SICS and PICS provide the capability for monitoring variables, including post-accident monitoring variables and system variables over their anticipated ranges for normal operation, for Anticipated Operational Occurrences, and for accident conditions as appropriate to meet the requirements of GDC 13. The PICS and SICS also provide a means of manual control capabilities for maintaining these variables and systems within prescribed operating ranges.

The staff determined that the applicant did not originally demonstrate sufficient reliability of the data communication systems required to support the functionality of PICS to meet the requirements of GDC 13 and GDC 19. In order to complete the functions required by GDC 13 and GDC 19, equipment such as network switches and electrical and fiber optic cables are provided (as part of the PICS automation and HMI buses), which support data communication between PICS and other I&C systems. The staff determined that the applicant did not commit to provide sufficient quality and capacity of these network buses to support the data communication functions of PICS, as requested in RAI 286, Question 07.09-52. In a February 19, 2010, response to RAI 286, Question 07.09-52, the applicant stated that plant safety protection is provided by automatic operation of the PS, assuming no software common-cause failure, or automatic operation of the DAS in case the PS experiences a software CCF. The normal control systems that will be utilized in the U.S. EPR must have adequate bandwidth to reliably operate and maneuver all the other systems in the reactor plant needed for plant operation and also to keep the plant reliably online. These I&C systems will be specified and procured consistent with the application of digital control technology currently in use in other power generation facilities. The ability of the automation and HMI buses to support PICS functions is verified during start-up testing. FSAR Tier 2, Section 14.2.12.11.6 (Test No. 129), describes PICS start-up testing. In RAI 442, Question 07.09-66, the staff requested that the applicant provide additional design descriptions to verify that the PICS has adequate bandwidth to accomplish functions required to meet GDC 13 and GDC 19. In a November 19, 2010, response to RAI 442, Question 07.09-66, the applicant proposed to include design commitments for the PICS and PAS to provide for adequate bandwidth to reliably operate and maneuver the process systems in the reactor plant needed for plant operations. In a June 22, 2011, response to RAI 442, Question 07.01-26, the applicant provided FSAR Tier 2, Section 7.1.1.3.2 mark-ups to include this proposed design commitment. In addition, this section provided additional requirements for the design of the PICS automation bus, HMI bus, and the DCS systems connected to the bus. This section states that sound engineering and design practices will be applied to the development of the PICS automation bus, HMI bus, and the DCS systems connected to the bus, and the PICS will be designed to have bandwidth to reliably operate plant process systems. The applicant extended this design commitment to the RCSL and PAS as described in FSAR Tier 2, Sections 7.1.1.4.5 and 7.1.1.4.6, respectively. The staff concludes that the proposed design criteria to have adequate bandwidth in the PICS, RCSL, and PAS to reliably operate plant process systems needed for plant operation are sufficient, as stated in the, respective FSAR Tier 2, Sections 7.1.1.3.2, 7.1.1.4.5 and 7.1.1.4.6, Interim Revision 3 mark-ups. The staff finds these commitments adequate to meet the requirements GDC 13 and GDC 19.

FSAR Tier 2, Section 7.1.1.4.7 states that the TG I&C system regulates the operation of the turbine-generator for power generation. The TG I&C system provides speed and load control, as well as control of TG auxiliaries. In RAI 286, Question 07.09-67, the staff requested that the applicant demonstrate that the overspeed control of the TG I&C system does not use the plant automation and HMI bus. In a December 18, 2009, response to RAI 286, Question 07.09-67, the applicant stated that the overspeed control of the TG I&C system does not use the automation and HMI buses and does not require input via the automation and HMI buses to

perform its function, as stated in FSAR Tier 2, Section 10.2.2.9. Based on the fact that the applicant does not require inputs or use the automation and HMI buses for the overspeed control of the TG I&C system, the staff finds this response acceptable. However, as required by 10 CFR Part 50, Appendix A, GDC 20, the applicant did not demonstrate that upon a reactor trip, initiated either manually by the operator or automatically by the PS or the DAS, reliable communication pathways between the PS and the TG I&C system, and between the DAS and the TG I&C system, exist, to ensure that the TG I&C system receives the reactor trip signal. Therefore, in RAI 442, Question 07.09-67, the staff requested that the applicant address this issue. In a March 15, 2011, response to RAI 442, Question 07.09-67, the applicant stated that for the PS, an automatic or manual reactor trip results in a turbine trip signal being sent to the TG I&C system via four isolated hardwired outputs (one per division). For the DAS, an automatic or manual reactor trip generates a turbine trip signal sent directly to the TG I&C system via four hardwired output (one per division). This response also stated that FSAR Tier 2, Section 7.8.1.1.3 will be revised to include the description of the interface between the DAS and TG I&C for the turbine trip signal and FSAR Tier 2, Section 7.3.1.2.17, will be revised to describe the interface between the PS and the TG I&C. The staff finds the transmission of hardwired outputs from the PS or DAS to the TG I&C if a manual reactor trip or automatic reactor trip has occurred is adequate to meet the requirements of 10 CFR Part 50, Appendix A, GDC 20. and as such finds this response acceptable. Specifically, the staff finds the use of divisionalized hardwired interfaces precludes the effects of data transmission errors and provides a reliable pathway to send the turbine trip signal.

#### **7.9.5 Combined License Information Items**

No applicable items were identified in the FSAR. No additional combined license information items need to be included in FSAR Tier 2, Table 1.8-2, "U.S. EPR Combined License Information Items," for data communication systems.

#### **7.9.6 Findings and Conclusions**

The staff reviewed FSAR Tier 2, Section 7.1 and the associated technical and topical reports of FSAR Tier 2 for conformance to the regulatory requirements of 10 CFR Part 50 and 10 CFR Part 52 as they relate to data communications systems. Below is a summary of the staff's evaluation findings.

##### **Performance**

Based on the information provided in FSAR Tier 2 and its referenced documents, the staff concludes that the data communication systems used in support of I&C safety systems have fully satisfied the requirements of IEEE Std 603-1998, Clauses 5.5 and 4.j. Specifically, the staff finds the deterministic behavior of the TXS system, as described in Topical Report EMF-2110(NP)(A), Section 3.1.1.5 ensures adequate performance of the data communication system to accomplish its safety function to meet IEEE Std 603-1998, Clause 5.5. In addition, based on the response time analysis provided in Technical Report ANP-10309P, Revision 3, Appendix B, the proposed modifications to clarify the term "I&C delay" to include PACS delay, and the response time testing and analysis ITAAC in FSAR Tier 1, Table 2.4.1-7, Item 4.24, the staff finds that the PS data communication is sufficient to address the requirements of IEEE Std 603-1998, Clause 4.j.

## Reliability

Based on the information provided in FSAR Tier 2, and its referenced documents, the staff concludes that the data communication systems used in support of I&C safety systems satisfied the requirements of IEEE Std 603-1998, Clause 5.15. Based on the use of cyclic processing without the use of process driven interrupts enables deterministic data communication for U.S. EPR I&C safety systems to meet the requirements of IEEE Std 603-1998, Clause 5.15.

## Effects of Data Storms

Based on the information provided in FSAR Tier 2 and its referenced documents, the staff concludes that the applicant has addressed the effects of data storms to demonstrate that the automation and HMI buses will be sufficiently reliable to support the functions required by GDC 13. Specifically, based on the commitment to include design criteria in FSAR Tier 2, Section 7.1.1.3.2, to withstand data storm and the interfacing DCS systems will be designed with thresholds for network traffic that are consistent with maximum data rates of the buses, the staff finds that the applicant has addressed the effects of network data storms.

## Control of Access

Based on the information provided in FSAR Tier 2 and its referenced documents, the staff concludes that the U.S. EPR I&C data communication systems design has not fully met the requirements of IEEE Std 603-1998, Clause 5.9. Specifically, in RAI 505, Question 07.09-72, the staff requested that the applicant describe the method used to prevent connection of the SU to more than one safety division at a time, given that a separate isolation switch and SU are used for the RPMS. In addition, in RAI 506, Question 14.03.05-34, the staff requested that the applicant describe whether a CPU state switch exist at the RPMS cabinet to restrict software modification to the RPMS and provide an ITAAC to verify this feature in the as-built system. **RAI 505, Question 07.09-72 and RAI 506, Question 14.03.05-34 are being tracked as an open items.**

## Single Failure Criterion

Based on the staff's evaluation of the information presented in FSAR Tier 2, Chapter 7, as supplemented by Technical Report ANP-10309P, the staff finds the applicant adequately demonstrated that the data communication systems in support of U.S. EPR safety systems meet IEEE Std 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21, by providing sufficient redundancy or alternative means to prevent loss of safety functions due to a single failure. The staff's evaluation is documented in Section 7.9.4.4.1 of this SER.

## Protection System Failure Modes

Based on the information provided in FSAR Tier 2 and its referenced documents, the staff concludes that the I&C data communication systems design has fully satisfied the requirements of 10 CFR Part 50, Appendix A, GDC 23. The staff finds the communication failures and mitigation strategies identified in Technical Report ANP-10309P, Appendix A, Table A.1.1 are adequate to conclude that communication failures within TXS based systems are mitigated by features within the system. The staff's evaluation is documented in Section 7.9.4.4.2 of this report.



## Independence between Redundant Portions of Safety Systems

Based on the information provided in FSAR Tier 2 and its referenced documents, the staff concludes that the U.S. EPR I&C data communication systems design does not fully meet the requirements of IEEE Std 603-1998, Clause 5.6.1. Specifically, the applicant has not demonstrated that the implementation of data communication between redundant divisions of U.S. EPR I&C safety systems has fully addressed the 20 interdivisional communication criteria in Section 1 of D I&C ISG-04 or provided an acceptable alternative to meet the requirements of IEEE Std 603-1998, Clause 5.6.1, as described in Section 7.9.4.5.1 of this report.

## Independence Between Safety Systems and Design Basis Events

IEEE Std 603-1998, Clause 5.6.2 specifies that one way to demonstrate independence between safety systems and design basis events is to demonstrate sufficient equipment qualification in accordance with the requirements specified in IEEE Std 603-1998, Clause 5.4. The staff's evaluation of the I&C data communication systems to the requirements of IEEE Std 603-1998, Clause 5.6.2, and 10 CFR Part 50, Appendix A, GDC 22, is completed as part of the evaluation of the overall U.S. EPR I&C safety system's satisfaction of the equipment qualification requirements specified in IEEE Std 603-1998, Clause 5.4. This is evaluated in Section 7.1.4 of this report.

## Independence between Safety Systems and Other Systems

Based on the information provided in FSAR Tier 2 and its referenced documents, the staff concludes that the U.S. EPR I&C data communication systems design does not fully meet the requirements of IEEE Std 603-1998, Clause 5.6.3, and 10 CFR Part 50, Appendix A, GDC 24. Specifically, the applicant has not demonstrated that the implementation of bi-directional communication between safety and non-safety systems within the U.S. EPR I&C systems has fully addressed the 20 criteria for communication independence in D I&C ISG-04, Section 1, or provided an acceptable alternative to meet the requirements of IEEE Std 603-1998, Clause 5.6.3, and 10 CFR Part 50 Appendix A, GDC 24, as described in Section 7.9.4.5.3 of this report.

## Capability for Testing and Calibration

The staff's evaluation of the data communications systems capability for testing and calibration to meet the requirements of the IEEE Std 603-1998, Clause 5.7, is completed as part of the evaluation of the overall U.S. EPR safety I&C systems' capability for testing and calibration, as documented in Section 7.1.4 of this report.

## Control Systems Data Communications Functions

The staff concludes that the proposed design criteria to have adequate bandwidth in the PICS, RCSL, and PAS to reliably operate plant process systems in the reactor plant needed for plant operation are sufficient and adequate to meet the requirements of GDC 13 and GDC 19.

## Protection System Function

The staff finds the transmission of hardwired outputs from the PS or DAS to the TG I&C to initiate a turbine trip once a manual reactor trip or automatic reactor trip has occurred is adequate to meet the requirements of 10 CFR Part 50, Appendix A, GDC 20. Specifically, the staff finds the use of divisionalized hardwired interfaces precludes the effects of data

transmission errors and provides a reliable pathway to send the turbine trip signal. The staff's evaluation is documented in Section 7.9.4.6 of this report.

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
Definitions		
<p>Definition of Common-cause Failure</p> <p>(Not included in IEEE Std 603-1991)</p>	<p>Definition of Common-cause Failure</p> <p>3.10 common-cause failure. Multiple failures attributable to a common cause.</p>	<p>IEEE Std 603-1998 contains a definition for “common cause failure,” but IEEE Std 603-1991 does not have a definition. Additional discussion on the acceptability of the definition is discussed below in the paragraph “IEEE Std 603-1998 Clause 5.16, Common Cause Failure Criteria.”</p> <p>The definition of common-cause failure does not reduce the acceptable level of quality and safety when IEEE Std 603-1998 is used in lieu of IEEE Std 603-1991; therefore, the staff considers the proposed alternative provides an acceptable level of quality and safety.</p>
<p>Definition of Components</p> <p>Discrete items from which a system is assembled. Note: Examples of components are wires, transistors, switches, motors, relays, solenoids, pipes, fittings, pumps, tanks, or valves.</p>	<p>Definition of Components</p> <p>3.11 Components</p> <p>Discrete items from which a system is assembled. Note: Examples of components are wires, transistors, switches, motors, relays, solenoids, pipes, fittings, pumps, tanks, or valves, computer programs, computer, hardware, or computer firmware.</p>	<p>IEEE Std 603-1998, Clause 3.11 expands the definition for the term “component” by adding the following examples of digital computer examples, “computer programs, computer, hardware, or computer firmware.”</p> <p>This additional wording in the definition of “component” does not reduce the acceptable level of quality and safety when IEEE Std 603-1998 is used in lieu of IEEE Std 603-1991. Additional discussion on the acceptability of the definition is discussed below in the paragraph “IEEE Std 603-1991 Clause 5.11 Identification, IEEE Std 603-1998 Clause 5.11 Identification.”</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>Definition of Detectable Failures</p> <p>detectable failures. Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures. Note: Identifiable but nondetectable failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication. Refer to IEEE Std 379-1988.</p>	<p>Definition of Detectable Failures</p> <p>3.13 detectable failures. Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures. Note: Identifiable but non-detectable failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication. Refer to IEEE Std 379-1994.</p>	<p>The words in IEEE Std 603-1998 referencing IEEE Std 379-1994 are not a rulemaking requirement and therefore do not change any of the requirements in IEEE Std 603-1991 or in IEEE Std 603-1998. The proposed alternative provides an acceptable level of quality and safety.</p>
<p>Definition of Division</p> <p>division. The designation applied to a given system or set of components that enables the establishment and maintenance of</p>	<p>Definition of Division</p> <p>3.14 division. The designation applied to a given system or set of components that enables the establishment and maintenance of physical,</p>	<p>IEEE Std 603-1998 added the statement, "NOTE - A division can have one or more channels," which clarifies that a division can consist of more than one channel. The clarification is acceptable. As seen in the table below, there are two clauses, Clause 5.11 and Clause 6.2, in which "division" or "divisional" is used and both clauses are identical in IEEE Std 603-1991 and IEEE Std 603-1998. The clarification does not change the requirements of the standard, nor does the clarification reduce</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>physical, electrical, and functional independence from other redundant sets of components.</p> <p>5.11 identification (4) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.</p> <p>6.2 Manual Control 6.2.1 Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.</p>	<p>electrical, and functional independence from other redundant sets of components. NOTE - A division can have one or more channels.</p> <p>5.11 identification d) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.</p> <p>6.2 Manual Control Means shall be provided in the control room to a) implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.</p>	<p>the acceptable level of quality and safety when IEEE Std 603-1998 is used in lieu of IEEE Std 603-1991. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>Definition of Safety System</p> <p>safety system</p> <p>Note: The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E.</p>	<p>Definition of Safety System</p> <p>3.25 safety system</p> <p>Notes: (1) The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E.</p> <p>(2)-This definition of “safety system” agrees with the definition of “safety-related systems” used by the American Nuclear Society (ANS) and IEC 60231A.</p>	<p>IEEE Std 603-1998 adds the wording, “This definition of “safety system,” agrees with the definition of “safety-related systems” used by the American Nuclear Society and IEC 60231A.” The addition of the wording does not change the requirements of the standard. Furthermore, the words that reference IEC 60231A, which is an International Electrotechnical Commission standard, are not a rulemaking requirement and, therefore, do not change any of the requirements. The added wording does not reduce the acceptable level of quality and safety when IEEE Std 603-1998 is used in lieu of IEEE Std 603-1991. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>
<p>IEEE Std 603-1991, Clause 4.5,      IEEE Std 603-1998, Clause 4 Item e</p> <p>Equivalence of Proactive actions to protective functions</p>		
<p>Clause 4.2 The safety functions and corresponding protective actions of the execute features for each design basis event.</p>	<p>Clause 4 Item b) The safety functions and corresponding protective actions of the execute features for each design basis event.</p>	<p>The words in IEEE Std 603-1998 which reference IEEE Std 497-1981 are not a rulemaking requirement and, therefore, do not change the requirement. The words, “protective actions identified in item b) that may be controlled,” as well as “The proactive actions are as follows,” as found in IEEE Std 603-1998, are equivalent in meaning to, “The following minimum criteria for each action identified in 4.2 whose operation may be controlled,” as found in IEEE Std 603-1991. They are equivalent in meaning for the following reason: Item 4.b as found in IEEE Std 603-1998, and 4.2 as found in IEEE Std 603-1991, both state, “The safety functions and corresponding protective actions of the execute features for each design basis event,” and, in addition, the list following, “The proactive actions,” as found in</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
		IEEE Std 603-1998, which lists items “1) , 2), 3), and 4),” are the same as the list in IEEE Std 603-1991.
<p>Clause 4.4 The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.</p>	<p>Clause 4 Item d) The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.</p>	<p>The requirements of IEEE Std 603-1998, Clause 4. Item e) are the same as IEEE Std 603-1991, Clause 4.5. This item requires that the design basis documentation include the minimum criteria for each protective action in Clause 4, Item b) whose operation may be controlled by manual means initially or subsequent to initiation. Since the requirements of IEEE Std 603 1998, Clause 4. Item e) are the same as IEEE Std 603-1991, Clause 4.5, the proposed alternative provides an acceptable level of quality and safety.</p>
<p>Clause 4.5 The following minimum criteria for each action identified in 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. See IEEE Std 494-1974.</p>	<p>Clause 4 Item e) The protective actions identified in item b) that may be controlled by manual means initially or subsequently to initiation. See IEEE Std 497-1981. The proactive actions are as follows:</p>	
<p>Clause 4.5.1 The points in time and the plant</p>	<p>Clause 4 Item e) 1)  The points in time and the</p>	

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
conditions during which manual control is allowed.	plant conditions during which manual control is allowed.	
Clause 4.5.2 The justification for permitting initiation or control subsequent to initiation solely by manual means.	Clause 4 Item e) 2)  The justification for permitting initiation or control subsequent to initiation solely by manual means.	
Clause 4.5.3 The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.	Clause 4 Item e) 3)  The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.	
Clause 4.5.4 The variables in 4.4 that shall be displayed for the operator to use in taking manual action	Clause 4.5.4 The variables in 4.4 that shall be displayed for the operator to use in taking manual action	
Clause 5.1 - Single-Failure Criterion		
systems shall perform all safety functions required for a design basis event in the presence of: (1) Any single detectable failure within the safety systems concurrent	The safety systems shall perform all safety functions required for a design basis event in the presence of: (a) Any single detectable failure within the safety	The addition of the wording in the IEEE Std 603-1998, "The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function," clarifies that a single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function. This clarification is acceptable.



IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1988 provides guidance on the application of the single-failure criterion.</p>	<p>systems concurrent with all identifiable but non-detectable failures, (b) all failures caused by the single failure, (c) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1994 provides guidance on the application of the single-failure criterion. IEEE Std 7-4.3.2-1993 addresses common cause failures for digital computers.</p>	<p>The words in the IEEE Std 603-1998 that reference IEEE Std 379-1994, and IEEE Std 7-4.3.2-1993 are not a rulemaking requirement and, therefore, do not change the requirement.</p> <p>Clause 5.1 requires that the safety system be able to perform its safety function required for a design basis event in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety. The clarification on single failure is acceptable, and otherwise the requirements of IEEE Std 603-1998, Clause 5.1 are the same as IEEE Std 603-1991. Clause 5.1. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>
<p>Clause 5.3 - Quality</p>		
<p>. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment</p>	<p>Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be</p>	<p>The reference to, "ASME NQA-1-1994," is not a rulemaking requirement and, therefore, does not change the requirement.</p> <p>Clause 5.3 states that the components and modules within the safety system be of a quality that is consistent with minimum</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQA1-1989).	designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (See ASME NQA-1-1994).	maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. The requirements of IEEE Std 603-1998, Clause 5.3, are worded the same as IEEE Std 603-1991, Clause 5.3. Therefore, the proposed alternative provides an acceptable level of quality and safety.
Clause 5.4 - Equipment Qualification		
Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.	Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.  Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE	The reference to the guidance in IEEE Std 7-4.3.2-1993 is not a rulemaking requirement and therefore does not change the requirement.  Clause 5.4 requires that safety system equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting the performance requirements as specified in the design basis. The requirements of IEEE Std 603-1998, Clause 5.4, are worded the same as IEEE Std 603-1991, Clause 5.4. Therefore, the proposed alternative provides an acceptable level of quality and safety.

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
	Std 7-4.3.2-1993.	
Clause 5.5 - System Integrity		
The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.	<p>The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.</p> <p>Guidance on the application of this criterion for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.</p>	<p>The reference to the guidance in IEEE Std 7-4.3.2-1993 is not a rulemaking requirement and, therefore, does not change the requirement.</p> <p>Clause 5.5 requires that the safety systems be designed to accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. The requirements of IEEE Std 603-1998, Clause 5.5 are worded the same as IEEE Std 603-1991, Clause 5.5. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>
Clause 5.6.3.2 - Equipment in Proximity		
(1) Separation: Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems'	a) Separation. Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to	<p>The reference to, "IEEE Std 384-1992," is not a rulemaking requirement and therefore does not change the requirement.</p> <p>This clause states that equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, will be physically separated from the safety system equipment to the degree necessary to retain the safety systems capability to accomplish their safety functions in the event of the failure of non-safety equipment, and that physical separation may be achieved by physical barriers or acceptable separation distance.</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981.</p>	<p>accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1992.</p>	<p>This clause further states that the physical barriers used to effect a safety system boundary shall meet the requirements of Clauses 5.3, "Quality," 5.4, "Equipment Qualification," and 5.5, "System Integrity," for the applicable conditions specified in Clause 4 Items g) and h) of the design basis. The requirements of IEEE Std 603-1998, Clause 5.6.3.2, are the same as IEEE Std 603-1991, Clause 5.6.3.2. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>
<p>Clause 5.6.3.3 - Effects of a Single Random Failure</p>		
<p>Where a single random failure in a no safety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1988 for the application of this</p>	<p>Where a single random failure in a non-safety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1994 for the application of this requirement.</p>	<p>The words in IEEE Std 603-1998, which reference IEEE Std 379-1994, are not a rulemaking requirement and, therefore, do not change the requirement.</p> <p>Clause 5.6.3.3 states that where a single random failure in a non-safety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. The requirements of IEEE Std 603-1998, Clause 5.6.3.3, are the same as IEEE Std 603-1991, Clause 5.6.3.3. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
requirement.		
Clause 5.6.4 - Detailed Criteria		
IEEE Std 384-1981 provides detailed criteria for the independence of Class 1E equipment and circuits.	IEEE Std 384-1992 provides detailed criteria for the independence of Class 1E equipment and circuits. IEEE Std 7-4.3.2-1993 provides guidance on the application of this criterion for the separation and isolation of the data processing functions of interconnected computers.	<p>The words in IEEE Std 603-1998 which reference IEEE Std 384-1992 and IEEE Std 7 4.3.2 1993 are not a rulemaking requirement and, therefore, do not change the requirement.</p> <p>The requirements of IEEE Std 603-1998, Clause 5.6.4 are worded the same as IEEE Std 603-1991, Clause 5.6.4. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>
Clause 5.11 - Identification		
Discrete items from which a system is assembled. Note: Examples of components are wires, transistors, switches, motors, relays, solenoids, pipes, fittings, pumps, tanks, or valves.	Discrete items from which a system is assembled. Note: Examples of components are wires, transistors, switches, motors, relays, solenoids, pipes, fittings, pumps, tanks, valves, computer programs, computer, hardware, or computer firmware.	<p>The words in IEEE Std 603-1998 which reference IEEE Std 384-1992 and IEEE Std 420-1982 are not a rulemaking requirement and, therefore, do not change the requirement.</p> <p>Clause 5.11 states that safety system equipment be distinctly identified for each redundant portion of a safety system, that identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes, that identification of safety system equipment and its divisional assignment shall not require frequent use of reference material, and that the associated documentation shall be distinctly identified. However, components or modules mounted in equipment or assemblies that are clearly identified as being in</p>
5.11 Identification.	5.11 Identification	

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:</p> <p>(1) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981 and IEEE Std 420-1982.</p> <p>(2) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.</p>	<p>In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:</p> <p>(a) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1992 and IEEE Std 420-1982.</p> <p>(b) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.</p> <p>(f) The versions of computer hardware, programs, and software shall be distinctly</p>	<p>a single redundant portion of a safety system do not themselves require identification. The additional wording in IEEE Std 603-1998, Item f, indicates that versions of computer hardware, programs, and software shall be distinctly identified. IEEE Std 603-1998, Clause 3.11, explains the definition for the term “component” by adding the following examples of digital computer examples, “computer programs, computer, hardware, or computer firmware.” This additional wording in the definition of “component” does not reduce the acceptable level of quality and safety when IEEE Std 603-1998 is used in lieu of IEEE Std 603-1991. Additionally, the expanded definition of “component,” when combined with Clause 5.11, Item b, is not to be interpreted that computer programs and firmware do not need to be identifiable,- per new Clause 5.11, Item f. Otherwise, the requirements of IEEE Std 603-1998, Clause 5.11, are the same as in IEEE Std 603-1991, Clause 5.11. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>
Clause 5.13 - Multi-Unit Stations		
The sharing of structures, systems, and components between units at multi-unit	The sharing of structures, systems, and components between units at multi-unit	The differences in wording do not change the requirements. The words in IEEE Std 603-1998 that reference IEEE Std 308-1991 and IEEE Std 379-1994 are not a rulemaking requirement and,

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1980. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1988.</p>	<p>generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1991. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1994.</p>	<p>therefore, do not change the requirement.</p> <p>Clause 5.13 states that the sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. The requirements of IEEE Std 603-1998, Clause 5.13, are the same as IEEE Std 603-1991, Clause 5.13. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>
<p>Clause 5.15 - Reliability</p>		
<p>For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.</p>	<p>For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.</p> <p>Guidance on the application of this criterion for safety system</p>	<p>The differences in wording do not change the requirements. The words in IEEE Std 603-1998 that reference IEEE Std 7-4.3.2-1993 are not a rulemaking requirement and, therefore, do not change the requirement.</p> <p>Clause 5.15 states that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. The requirements of IEEE Std 603-1998, Clause 5.15, are the same as IEEE Std 603-1991, Clause 5.15. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
	equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.	
Clause 5.16 - Common Cause Failure Criteria		
(Not included in IEEE Std 603-1991)	Plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure (See IEEE 379-1994). IEEE Std 7-4.3.2-1993 provides guidance on performing an engineering evaluation of software common cause failures, including use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the common cause failure.	<p>IEEE Std 603-1998 contains a requirement for “common cause failure criteria,” but IEEE Std 603-1991 does not have an equivalent requirement.</p> <p>Clause 5.16 requires that plant parameters be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure. IEEE Std 603-1998 provides a definition of “common-cause failure” as multiple failures attributable to a common cause. Clause 5.16 also refers to IEEE Std 379-1994 and IEEE Std 7-4.3.2-1993 for additional guidance on performing an engineering evaluation of software common cause failures, including use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the common cause failure. Since Clause 5.16 is an additional criteria beyond that contained in IEEE Std 603-1991, adding this criteria does not reduce the acceptable level of quality and safety when IEEE Std 603-1998 is used in lieu of IEEE Std 603-1991. Therefore, the proposed alternative provides an acceptable level of quality and safety</p>
Clause 6.8 - Setpoints		



IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>Clause 4.4 The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.</p> <p>6.8 Setpoints</p> <p>6.8.1 The allowance for uncertainties between the process analytical limit documented in Section 4.4 and the device setpoint shall be determined using a documented methodology. Refer to ISA S67.040-1987.</p> <p>6.8.2 Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating</p>	<p>Clause 4, Item d) The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.</p> <p>6.8 Setpoints.</p> <p>The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.</p> <p>Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or</p>	<p>The words in IEEE Std 603-1998 which reference are not a rulemaking requirement and, therefore, do not change the requirement.</p> <p>The wording in IEEE Std 603-1998, Clause 4, Item d, is the same as the wording in IEEE Std 603-1991, Clause 4.4. Clause 6.8 states that the allowance for uncertainties between the process analytical limit documented in Clause 4, Item d, and the device setpoint must be determined using a documented methodology, and where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design must provide a positive means of ensuring that the more restrictive setpoint is used when required. The requirements of IEEE Std 603-1998, Clause 6.8, are the same as IEEE Std 603-1991, Clause 6.8. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>

IEEE Std 603-1991	IEEE Std 603-1998	Discussion of Differences
<p>conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.</p>	<p>set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.</p>	
<p>Clause 8.1 - Electrical Power Sources</p>		
<p>Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1980.</p>	<p>Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1991.</p>	<p>The differences in wording do not change the requirements. The words in IEEE Std 603-1998 which reference IEEE Std 308-1991 are not a rulemaking requirement and, therefore, do not change the requirement.</p> <p>Clause 8.1 states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. The requirements of IEEE Std 603-1998, Clause 8.1, are the same as IEEE Std 603-1991, Clause 8.1. Therefore, the proposed alternative provides an acceptable level of quality and safety.</p>